THE IMPACT OF USERS' CHARACTERISTICS ON THEIR ABILITY TO DETECT PHISHING EMAILS

Ibrahim Mohammed Alseadoon

A thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

Science and Engineering Faculty

Queensland University of Technology

Brisbane – Australia

2014

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: QUT Verified Signature

Date: June 2014

Abstract

Phishing emails result in significant losses, estimated at billions of dollars, to both organisations and individual users (Herley & Florencio, 2008). Attempts to address the problem began with the first appearance of phishing emails in 1996 (James, 2006). These have included the development of new technological defences that detect phishing emails before they even reach their victims (Bergholz et al., 2008; Cook, Gurbani, & Daniluk, 2009; Fette, Sadeh, & Tomasic, 2007). None of these technological solutions, however, has been entirely successful. Accordingly, our research addresses non-technical aspects of the problem by investigating users themselves. While users have been targeted by educational programs, the focus of these programs has been on the technical side; for example, advising users not to respond to emails that include IP addresses in their links. The vulnerabilities of users themselves have received little attention. Therefore, there was a need to understand users' detection behaviour with phishing emails.

To reduce users' vulnerability to phishing emails, we need first to understand users' detection behaviour. To the best of our knowledge, no previous studies have investigated the full range of processes involved in this behaviour. Most research focuses on only one type of behaviour, namely, whether or not participants respond to phishing emails.

To better understand users' detection behaviour, we began by examining research into the cognitive process that users experience when they face phishing emails (Vishwanath, Herath, Chen, Wang, & Rao, 2011; Xun, Clark, & Jacob, 2008). This suggested that users' detection behaviour goes through more than one phase, but there has been little attempt to investigate users' detection behaviour from the beginning of the process of receiving and suspecting a phishing email. The extant literature fails to provide understanding of users' detection behaviour and the impact of users' characteristics on that behaviour. Our research aims to fill this gap.

The approach adopted in this empirical study is based on the theory of deception (Johnson, Grazioli, Jamal, & Glen Berryman, 2001; Johnson, Grazioli, Jamal, & Zualkernan, 1992) and on a model that allows this theory to be applied in a computer based environment (Grazioli, 2004). In order to examine users' detection behaviour and the impact of users' characteristics, the research had to engage participants in the process of detecting phishing emails. There was a need to 'lure' participants into an experiment that included sending phishing emails while ensuring that nothing in the study had the potential to jeopardise their safety (i.e. no harm would come to them from the phishing emails). Participants' behaviour (*responses*) to the phishing emails was recorded and they were classified into detectors and victims. A quantitative method was used to relate participants' characteristics with their behaviour and a qualitative method was used to generate in-depth understanding of participants' detection behaviour.

Of necessity, the study design itself involved an element of deception (Finn & Jakobsson, (2007), and we were sensitive to the ethical aspects of this. Informing participants in advance that they are participating in a phishing email study would have had a negative effect on the results, since they would be likely to increase their detection behaviour (Wright et al., 2009). Accordingly, the real nature of the research was not revealed to participants before they were sent phishing emails that we had developed. The study was carefully designed to ensure that valid data could be collected without harm to participants, and it was approved by the University's Ethics Committee.

The output of the research is a new model to explain the impact of users' characteristics on their detection behaviour. The model was tested through two studies in two different countries (Saudi Arabia and Australia), with a total of 780 participants. In addition to testing the model, these two studies helped to measure the impact of culture on users' detection behaviour. The final model was tested using structural equation modelling (SEM). The results showed that the proposed model explains 13% and 45%, respectively, of the variance in Saudi Arabian and Australian participants' tendency to respond to phishing emails.

The results also showed that users' characteristics (individual factors) play an important role in affecting the three main phases in users' detection behaviour:

susceptibility, confirmation and response. Specifically, high trust, high submissiveness and low perceived email richness significantly increase users' susceptibility (first phase). Choosing poor confirmation channels and consulting unqualified persons decrease users' confirmation (second phase). High susceptibility, a weak confirmation phase and certain personality traits significantly increase users' response to phishing emails (final phase).

Another important finding is that phishing email victims fall into three main categories: naive victims, who have low suspicion; doubtful victims, who suspect phishing emails but fail to confirm their suspicion; and risk-taker victims, who ignore warnings about phishing emails. Different strategies are needed to address the specific vulnerabilities of each type of victim. The ability to identify potential victims is of considerable benefit to both organisations and individual users in the quest to solve the problem of phishing emails.

Acknowledgements

First and foremost, my grateful thanks goes to my God "Allah – الله" for giving me the courage and strength to finish my PhD studies despite the many difficulties encountered along the way. There were times when I felt that I had reached a dead end, but Allah gave me the strength to continue.

I am also grateful to my family. I thank my mother for her support and prayers throughout my life and in my studies. My wife Sumayyah has been a great support throughout my postgraduate studies and has shared all the hard times with me. My two delightful children, Arreem and Alwaleed, filled the long distance from the rest of my original back home. I thank Allah every day for this great privilege. Finally, my thanks go to my niece Adeem, who taught me, without her knowing it, that life is full of failures on the way to your goal but you will succeed if you don't give up.

I would also like to express my deep appreciation to my academic colleagues. My principal supervisor, Dr Taizan Chan, believed in my ability to complete the PhD journey and guided me throughout. There were times when I struggled to complete the project and his support at these times was invaluable. I would also like to thank my associate supervisor, Dr Ernest Foo, and all my colleagues at QUT, especially M. F. I. Othman and Fayez Alqahtani, for their cheerfulness and support. Thanks to my friend and colleague Jazem Alanazi at Wollongong University for his support and information sharing, which helped both of us to get through this PhD journey.

I would like to thank my government and all its agencies for sponsoring my study through the University of Ha'il. I am also grateful to the Australian government for providing a suitable environment for living and studying here. Thanks to all my friends and neighbours in Brisbane, specifically in Oxley, for the wonderful time I spent with them during my time away from my homeland.

Table of Contents

Contents

List of Tables

List of Figures

List of Abbreviations

MDD	Model of detecting deception
Trust	Users' disposition to trust
Missive	Users' submissiveness
Email_Exp	Perceived email experience
Email_Rich	Perceived email richness
Channel	Used confirmation channel
Y_Internt	Number of years using the Internet
H_Internt	Number of hours using the Internet per day
Y_Email	Number of years using the email service
Y_Uni	Number of years using the university email service
No_Emails	Number of emails received per day
Activity	The type of activity on the Internet (surfing, social, transaction)
Detector	A user who manages to open and ignore the phishing email
Victim	A user who responds to the phishing email

Refereed Conference Papers

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012). *Who is more susceptible to phishing emails? A Saudi Arabian study.* Paper presented at the ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012, Geelong, Victoria, Australia.

Alseadoon, I, Othman, M.F., Foo, E., & Chan, T., (2013). *Typology of Phishing Email Victims Based on their Behavioural Response.* Paper presented at the 19th American Conference on Information Systems (AMCIS 2013), Chicago, Illinois, USA.

Alseadoon, I, Othman, M.F., & Chan, T., (2014). *What is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?.* Paper presented at the 1st International Conference on Communication and Computer Engineering (ICOCOE2014), Malacca, Melaka, Malaysia.

Keywords

Susceptibility: Refers to the first phase in users' detection behaviour. Susceptibility is the opposite of suspicion. High susceptibility means that users have less suspicion towards phishing emails, and vice versa.

Confirmation channels: Refers to those channels that users choose to confirm or refute their suspicions about phishing emails.

Response: Refers to the last phase in detection behaviour when users decide to perform the action requested in the phishing emails.

Detectors: Those users, who open the phishing email, evaluate its authenticity and decide to ignore it.

Victims: Those users who respond to phishing emails by complying with the embedded request.

Rich medium: A medium that carries several cues. An example is face-to-face interaction, which can convey eye movement, body language and voice tone. In contrast, email is considered a poor medium because it contains a very limited number of cues.

Chapter 1: Introduction

This chapter presents the background to the research and provides a detailed discussion of the research focus. The aim and significance of the study are explained and the organisation of the thesis is described.

1.1 Background

Since the inception of the Internet, the number of users has grown dramatically because of its many practical applications in daily life. One of these is to connect users with businesses. The Internet provides businesses with the opportunity for growth through the provision of online services. Online services are attractive because they can connect users to businesses in distant locations and are available 24 hours a day, seven days a week. With this convenience, however, come potential security issues.

Online services that require a high level of security include banking and shopping. Because these online services often involve access to sensitive and private information, they require a similar level of security to that provided by their traditional counterparts. In traditional banking for example, customers are encouraged to check that the automatic teller machine (ATM) is legitimate and to ensure that their personal identification number (PIN) remains secret. The same conditions apply in online banking, where clients are encouraged to ensure that the website they are visiting is legitimate and not to disclose personal information such as passwords. Unfortunately, some users fail to satisfy these requirements and this has attracted criminal activity (Mannan & Oorschot, 2008).

One of the main forms of criminal activity that results from users' failure to satisfy security requirements is known as a phishing attack. Phishing attacks "exploit characteristics of human behaviour in order to increase the chances of the user doing what is desired" (Karakasiliotis, Furnell, & Papadaki, 2006).

Phishing attacks generally involve a method known as 'bait and hook' (Emm, 2006), in which phishing emails deceive users into connecting to phishing websites. The aim of these websites is to steal private information from users who connect to them. Phishing websites are harmless if no one connects to them. Therefore, their negative impact will be reduced if users can be prevented from complying with phishing emails. Unfortunately, users are not well prepared to defend themselves against phishing emails (Downs, Holbrook, & Cranor, 2007) and therefore become victims.

The number of phishing emails is extremely high. A recent study recorded around 156 million phishing emails per day (Get Cyber Safe, 2013). Since the purpose of these attacks is financial gain, they mainly target financial and payment services. These sectors received 70% of the reported attacks in the first quarter of 2013 (Anti-Phishing Working Group, 2013). It has been estimated that they result in an annual loss of between $2.4 million and $9.4 million per one million online customers in the banking sector alone (Trusteer, 2009).

Given the large number of attacks, the corresponding number of victims and associated losses is also high. Based on the number of phishing emails per day, the number of victims could reach 80,000 per day (Cyveillance, 2010). Overall, the estimated monetary loss from phishing attacks ranges from $61 million to approximately $3 billion per year (Herley & Florencio, 2008; Pettey, 2006). These are likely to be the minimum numbers involved, since they are based on reported attacks and losses. Globally, the actual figures could be much larger because not all attacks are reported

The large number of launched attacks, however, does not entirely account for the number of victims and associated losses. The success of phishing emails is also attributable to their clever design, which can trick even expert users with advanced technological knowledge (Aburrous, Hossain, Dahal, Bradford, & Thabatah, 2010). Adams (2012), for example, found that expert users who make careful and technical decisions about emails still fall victim to phishing emails. Clearly, general users with less knowledge of technology are even more vulnerable.

The problem of phishing emails becomes even more complex when consideration is given to differences among users. Such differences need to be taken into account when providing solutions and instruction. Phishing emails are not sent to specific individuals but *en masse*, which means that their recipients may come from different cultures. For example, a phishing email targeting the Queensland University of Technology (QUT) will not be limited to Australian students, since the university has a multicultural student body. Phishing emails target every user who owns an email account regardless of his or her background. It is an open question whether students from different cultures are similarly vulnerable. Our research investigates the impact of two different users from two different countries on their ability to detect phishing emails. Given both the scope and complexity of the problem, there is an urgent need to reduce the negative impact of phishing emails on users and organisations.

While some previous research has addressed this problem, most solutions that have been developed focus on preventing phishing emails from deceiving users (Hong, Kelley, Tembe, Murphy-Hill, & Mayhorn, 2013; Purkait, 2012). These solutions include tools that either detect phishing emails or warn users about them. Less research attention, however, has been paid to users' behaviour: What happens when these tools fail?

The following section explains in greater detail the focus of our research.

1.2 Research focus

Users are the focus in phishing email attacks. Phishing emails must deceive users to be successful. Users are targeted because they have been identified as the weakest link in the Internet security chain (Herzberg, 2009). The protection and exchange of confidential information in the Internet occurs in the trust path, which comprises three main elements: servers, transit channels and users (see Figure 1).

Confidential information is shared between servers and users through the transit channel, which authenticates users to servers. This means that whoever provides this information to servers will be granted the same access to online

services as authorised users would. Hence it is important to obtain this privileged information and perpetrators employ a variety of methods to do so. The Internet, however, is designed to make this as difficult as possible.

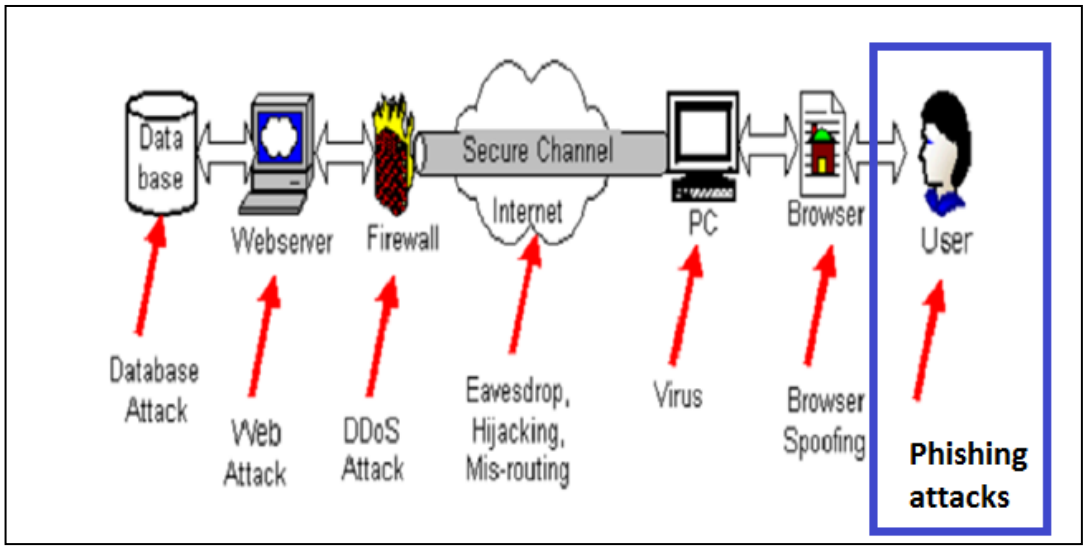

Figure 1: Trust path with various attacks (Li & Wu, 2003)

Protecting confidential information in these three elements is an important goal of Internet design. Servers employ advanced software to prevent confidential information from being accessed by an unauthorised entity. The transit channel protects the confidential information it carries using a protocol called Secure Sockets Layer (SSL) or Transport Layer Security (TLS) as a *de facto* form of protection (Oppliger, Hauser, & Basin, 2006). This protocol ensures that information exchanged between users and servers is encrypted inside the channel. Encryption prevents other parties from gaining access to it (Chomsiri, 2007). Users connect to the Internet via their devices (e.g. mobiles or laptops) to communicate with servers. Users can protect the confidential information entered into their computers by installing security programs such as anti-virus software. Of course, users themselves know their confidential information and this makes them a key target for perpetrators.

Unfortunately, users can be tricked into revealing this information (Dhamija, Tygar, & Hearst, 2006). Criminals deceive users into exposing their confidential information by leading them to believe that the phishing emails are legitimate. They do this by exploiting the gap between what users think they are connected to and

what they are actually connected to (Downs, Holbrook, & Cranor, 2006; Li & Wu, 2003; Wu, Miller, & Little, 2006). Phishing emails are effectively designed to make users think they are connected to a legitimate entity although they are actually connected to a malicious entity. There is an urgent need to stop users from legitimising phishing emails.

Many forms of prevention have already been devised. For example, education programs have targeted users to teach them how to identify phishing email cues[1] (Kumaraguru, 2007; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008). Others have focused on users' computers by providing tools that can distinguish between legitimate and illegitimate websites (Kim et al., 2008). Despite these innovations, users continue to fall victim to phishing emails (Jagatic, Johnson, Jakobsson, & Menczer, 2007; Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010) and perpetrators continue to find ways around these solutions. Accordingly, there is a need to approach the problem from a different perspective and examine why users fall prey to phishing emails in the first place. This non-technical perspective has been under-researched.

A substantial body of knowledge exists in relation to deception (lying). It has been shown that people are able to detect deception using non-technical cues. Of particular importance to the ability to detect deception are individual characteristics, such as experience, personality and culture, among others (Anderson, DePaulo, Ansfield, Tickle, & Green, 1999; Carlson, George, Burgoon, Adkins, & White, 2004; Miller & Stiff, 1993; Wright, Chakraborty, Basoglu, & Marett, 2009). These factors have not been thoroughly investigated in relation to the problem of phishing emails. Phishing emails employ the same principle of deception, that is, they lure users into erroneous conclusions. Therefore, findings from deception studies are potentially relevant to studies in the field of phishing emails. This project investigates whether the same factors that are relevant to detecting deceptive messages in conversations are also related to users' ability to detect phishing emails.

This work on deception, together with some previous research on phishing emails, suggests that there may be a connection between users' characteristics and users' detection behaviour. In particular, Wright et al. (2009) found from qualitative

[1] These are the signs that can identify phishing emails.

data that participants used non-technical means of evaluating the legitimacy of phishing emails. For example, one participant reported that he did not respond directly to the phishing email that requested private information but waited for the request to come directly from the lecturer before taking action (Wright et al., 2009). Unfortunately, the investigation did not pursue this important finding further.

Another potentially relevant factor is culture. Deception (lying) studies have found that users from different cultures have a high level of accuracy in detecting deception across cultures if the deception is conducted via a rich medium[2] such as video. By contrast, detection across cultures was found to be difficult when the deception was conducted in a poor medium such as voice recording (Bond, Omar, Mahmoud, & Bonser, 1990). Emails are considered to be a poor medium and this may affect users' ability to detect deception across cultures. Kumaraguru et al. (2009, 2009) conducted two similar experiments in two different cultures. The results showed different patterns in the factors affecting users' detection ability in the two experiments. This is discussed in more detail in Chapter 2.

Interesting demographic differences have been found between users who are detectors and those who are victims, but these have not been followed up by researchers. For example, studies whose main focus was on improving the efficiency of education programs have identified differences in users' demographics that affect their ability to detect phishing emails (Kumaraguru et al., 2009). Other studies have investigated demographics in relation to the design of phishing emails (Jagatic et al., 2007), but again the non-technical factors were not the primary focus. Moreover, previous studies failed to investigate users' detection behaviour[3] and its impact on their ability to detect phishing emails. Users do not automatically become victims of phishing emails and they apply different strategies to judge the authenticity of an email (Downs et al., 2006). There is currently little understanding in the literature of users' detection behaviour and the impact of users' characteristics on this behaviour.

Further research is needed to explain why users respond to phishing emails. If weaknesses in their detection behaviour can be identified, .these can be targeted to improve users' detection ability. The characteristics that impact on users' detection

[2] Rich medium refers to a medium that can convey several cues. The face-to-face medium, for example, conveys eye movement, body language and voice tone.
[3] Users' detection behaviour refers to users' behaviour when they encounter a phishing email.

behaviour should also be investigated. If there is an association between certain characteristics and a particular weakness, this would allow vulnerable users to be identified in advance to improve their defence against phishing attacks.

1.3 Aim and Significance of the Study

The aim of our research is to identify victims of phishing emails from their characteristics and their behavioural weaknesses in detecting phishing emails. The overall purpose is to improve users' protection against phishing emails.

To achieve this aim, the first task is to identify weaknesses in users' detection behaviour when they receive a phishing email. A review of the extant literature shows that most previous research on phishing emails has focused on whether or not users respond to phishing emails. There has been little investigation into the whole process of detection which contributes to users becoming victims or detectors. Therefore, we began by looking for research on phishing emails that is relevant to understanding users' detection behaviour.

Since there has been relatively little research specifically addressing the topic of users' detection behaviour, we explored studies that have investigated the cognitive process involved in decision-making about phishing emails in the last decades. These decisions are essential in making users behave in a certain way. Three main cognitive models have been used to illustrate the mental process of making decisions about phishing emails (see Section 2.3). For example, Grazioli's (2004) model identifies four phases in this process. There are differences between detectors and victims in these four phases (see Section 2.4). While the cognitive process sheds light on decision-making vulnerability, it does not fully explain why some users become victims. Other aspects of behaviour affect users' decisions, and these require further investigation.

Grazioli's model, which is applied in our research, identifies the cognitive phases that underpin users' deception detection behaviour. Decision-making does not occur instantly but progresses through different phases until the user makes the final choice of whether to respond to or ignore a phishing email request. Researchers who

focus on the final phase have missed the opportunity to identify other weaknesses that render users vulnerable to becoming victims. Understanding these weaknesses in users' detection behaviour is important if we are to help people avoid making costly mistakes.

There are several issues involved in measuring users' detection behaviour. Existing measurements are inadequate because they do not investigate the whole process of users' detection behaviour. Most studies have a specific focus on only one phase. These studies fall into two main categories: those that present participants with an image of a phishing email and ask them to choose an action (Jakobsson, Tsow, Shah, Blevis, & Lim, 2007; Sheng et al., 2010), and those which record users' behaviour after they have received a phishing email (respond or ignore) (Kumaraguru et al., 2008; Wright et al., 2009). These studies fail to investigate all of the detection behaviour involved in users' decision-making about phishing emails.

Studies in the first category (i.e. showing images of phishing emails) have several limitations. First, they involve asking a direct question about whether these images are phishing emails (Jakobsson et al., 2007; Karakasiliotis et al., 2006). This kind of question actually initiates the process of detection. Users who are asked to judge the legitimacy of phishing emails may not have suspected these emails in everyday life. In other words, this type of study begins from the first step in the detection process, whereas some users may not even get this far (see Section 4.8).

A second limitation arises from the request to choose a response (Downs et al., 2007; Sheng et al., 2010). This is a measure of users' intentions rather than of actual behaviour, and involves no potential risks (unlike the real life situation).

Finally, the study design requires users to make an immediate decision. In real life, however, users may see a phishing email and postpone their response until they receive the request in person (Wright et al., 2009). Therefore, this is not a suitable way of measuring final behaviour (i.e. whether users actually respond to or ignore phishing emails).

In the second category of studies, subjects' actions following receipt of a phishing email (i.e. final behaviour) are recorded. The limitation here is that these studies ignore those behaviours that occur before users reach this stage. Users do not

arrive at the final behaviour (respond or ignore) without interacting with the phishing email or being influenced by their own characteristics or knowledge. Our research avoids these issues by investigating the whole process of users' detection behaviour from beginning (spotting a phishing email) to end (final behaviour).

The impact of user characteristics, including cultural differences, is an important dimension that has been neglected in previous research. Phishing emails do not discriminate—any user with an email account is at risk. Our study takes these differences into account as factors that may impact on detection behaviour.

1.4 Research Questions

The following research questions informed our study design.

1. **What is the process of users' detection behaviour?**

Users who receive phishing emails fall into two categories: detectors and victims. It is important to investigate the differences between these two types. Clearly, they make different behavioural choices (ignore or respond). In order to explain this difference, we need first to compare their respective detection behaviour. As previously discussed, the literature lacks sufficient information to permit such comparison, since most research has focused on whether users respond to or ignore phishing emails

Accordingly, one of our research objectives is to identify the whole process of users' detection behaviour. In this way, detectors can be compared with victims to establish any differences between them and this, in turn, helps to identify the weaknesses in victims' detection behaviour. This knowledge is necessary for the development of appropriate preventative strategies.

2. **How can the process of detection help in differentiating phishing email victims?**

Victims of phishing emails are generally identified as those who respond to phishing emails. Our research, however, strongly suggests that the process of detecting phishing emails is not limited to one phase (i.e. respond or not). Rather, response is preceded by other phases, which also need to be investigated for weaknesses that make users vulnerable to a phishing attack. It is important to establish, for instance, whether victims share the same weakness or have different kinds of weakness.

If victims have different weaknesses in different phases, this suggests that there can be no 'one size fits all' preventative strategy. The literature proposes solutions that are expected to be equally effective for all victims, but experience shows that this is not the case. For example, education programs have proved successful in improving users' ability to detect phishing emails, but some people who receive these programs still become victims (Bekkering, Hutchison, & Werner, 2009; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010). Therefore, it is important to know whether victims share a common weakness or if there are several weaknesses that require attention.

3. **What is the impact of individual differences on the process of detection?**

After identifying users' detection behaviour, we need to identify differences between users themselves. We obtain that by investigating the impact of users' characteristics on their detection behaviour. As noted above, users' characteristics impact on their ability to detect deception in general, but their role in relation to phishing emails has received little research attention.

Our study will investigate users' characteristics and their impact on detection behaviour. The investigation is not limited to the final phase of detection behaviour (respond or ignore) but includes the whole process. This contributes to our goal of improving users' detection ability through non-technical means.

4. What is the impact of collective differences on the process of detection?

In broad terms, most citizens of a country share a common culture. Culture affects users' ways of thinking and behaving (Hofstede, 1993). Culture is an important source of difference between groups of users who may receive phishing emails. Therefore, this study seeks to identify the impact of culture on users' response to phishing emails. For example, would a phishing email that impersonates an Australian company or authority have the same effect on Australian and Middle Eastern users? Does a particular type of phishing email have the same response rate in different cultures? Phishing emails are sent to users who have email accounts, regardless of their cultural differences. Our study therefore investigates the impact of culture on users who receive similar phishing emails, as well as the influence of users' characteristics.

Better understanding the differences between detectors and victims allows us to identify the factors that need to be addressed in order to improve users' protection against phishing emails. Knowledge of victims' characteristics will also assist organisations to identify vulnerable users and deploy appropriate protective strategies.

1.5 Study Design

This study adopted a mixed methods approach to data collection. Both quantitative and qualitative methods were used because of their ability to provide a comprehensive overview of the problem. Quantitative data were collected about users' susceptibility[4] to phishing emails, users' characteristics and users' confirmation channels[5] (Research Questions 1 and 3). Quantitative data were collected to measure relationships between variables of relevance to our research. The experimental method involved users in actual detection behaviour with phishing

[4] Users' susceptibility refers to the first phase in users' detection behaviour.
[5] Confirmation channels are those channels that users choose to confirm or deny their suspicion about phishing emails.

emails (Research Questions 1, 2, 3 and 4), while the qualitative data generated in-depth insight into users' detection behaviour (Research Questions 1, 2, 3 and 4).

Question 4 relates to the impact of group differences represented by culture on users' detection process. Therefore, the research comprised two separate studies in two different cultures. The first study was conducted in Saudi Arabia and had a total of 350 participants. The second study was conducted in Australia and had a total of 430 participants.

1.6 Thesis Outline

Chapter 2 presents a critical review of the literature on phishing emails and identifies gaps in existing research-based knowledge. Chapter 3 describes the research model that underpinned the design of the present study. Chapter 4 presents a detailed account of the research methodology, which involved a mixed methods (quantitative and qualitative) approach. The quantitative analytic procedures and findings from the studies in Saudi Arabia and Australia are presented in Chapter 5. Chapter 6 describes the procedures used to analyse the qualitative data and presents findings from both studies. A detailed discussion of all results is provided in Chapter 7. Chapter 8 summarises the theoretical and empirical contributions of the study, identifies its limitations, and makes recommendations for future research.

1.7 Summary

This chapter has discussed the background to the present study and identified the research problem it addresses. The aim and significance of the research have been explained and the specific research questions that informed the study design have been elaborated. The chapter concluded with an overview of the thesis organisation.

Chapter 2: Literature Review

This chapter presents a critical review of literature relevant to the research topic. It defines phishing emails and describes their main design features, with particular attention to how these features are used to deceive users.

As well as technical dimensions, the review addresses users' decision-making in relation to phishing emails. Three key cognitive models of decision-making are examined with a view to identifying areas of vulnerability among users. The main theory employed in this research, the theory of deception, is explained and applied to an examination of differences between detectors and victims. Users' weaknesses in detecting phishing websites are explored to shed light on their vulnerability to phishing emails, which deploy similar technical tricks.

Next, various solutions that have been developed to tackle the problem of phishing emails are described and evaluated. The chapter concludes with a discussion of gaps in the knowledge base, with particular focus on users' detection behaviour and the influence of users' characteristics on the ability to detect phishing emails.

2.1 Phishing Emails: Overview

Phishing emails have been defined as those emails which employ both social engineering and technical tricks to steal secret information from users (Anti-Phishing Working Group, 2009) and which "exploit characteristics of human behaviour in order to increase the chances of the user doing what is desired" (Karakasiliotis et al., 2006). Thus phishing emails are characterised by exploitation and deception.

Phishing emails trick users by making them believe that they are revealing their secret information to a legitimate entity. Through their design, the senders impersonate legitimate organisations to convince users to comply with their request. A phishing attack relies on users' inability to distinguish between legitimate and

illegitimate entities. Believing that they are connected to the legitimate entity, users reveal their confidential information to access their account.

To be successful, these emails need to make users reveal their confidential information outside the trust path (see Figure 1), since information outside the trust path is not protected. By impersonating legitimate entities, they deceive users into thinking that they are using the trust path to submit this information. The deception is perpetrated in two ways: through click action or reply action. Click action involves a request for the user to visit a phishing website in order to steal their confidential information (see Figure 2). Reply action involves a request for the user to reply by sending their secret information to these emails (see Figure 3). The design features of these deception techniques are discussed in more detail in the following sections.

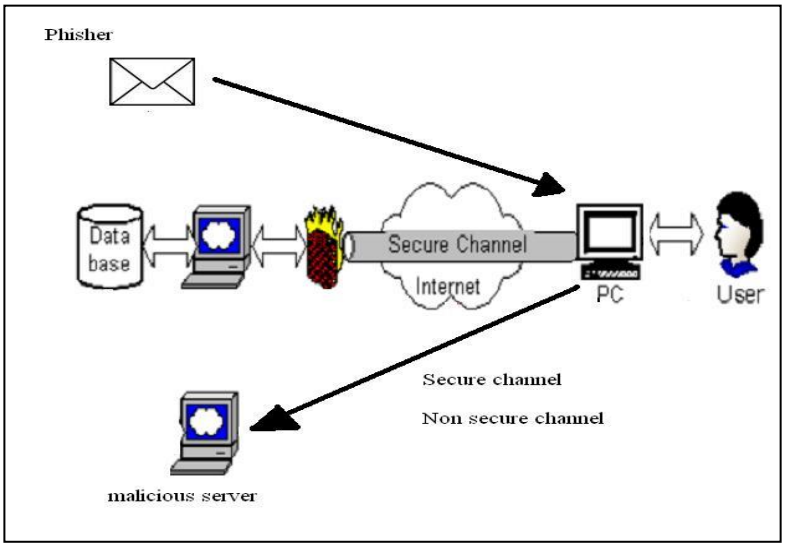

Figure 2: Phishing email click action

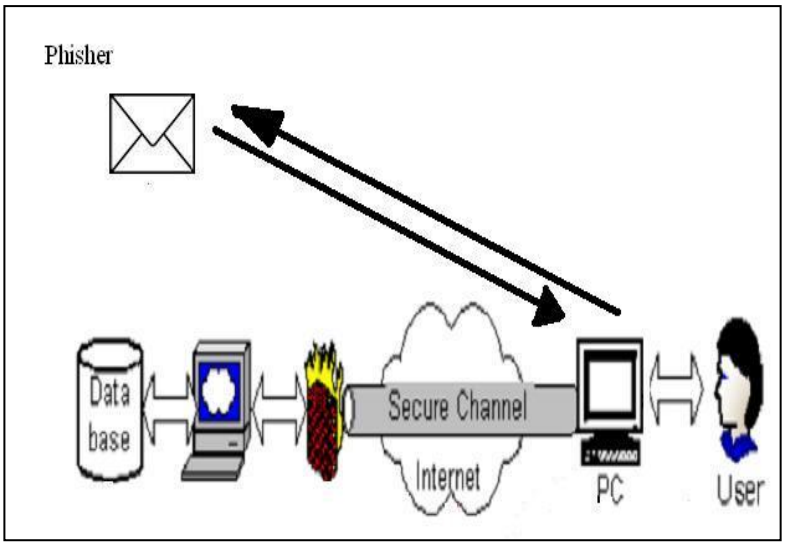

Figure 3: Phishing emails reply action

2.2 Design Features of Phishing Emails

This section explains the design features that phishing emails employ to make them appear credible and which we used in the design of our own phishing emails (see Section 4.6.1). This discussion draws on two main studies (Wang et al., 2009; Sharma, 2010) that examined these techniques.

2.2.1 Alleviating suspicion

Wang et al. (2009) analysed 195 phishing emails using the elaboration likelihood model (ELM) (Petty & Cacioppo, 1986). The ELM explains how users make decisions (see Section 2.3.3). The findings show that phishing emails are well designed to reduce users' suspicion and comply with their request.

For example, the ELM proposes that the quality of the message's argument strongly influences the receiver's attitude towards message acceptance. Argument quality refers to the strength of conviction in the argument that is embedded in the message (Bhattacherjee & Sanford, 2006). Message acceptance is necessary if the phishing attack is to succeed. For example, a phishing email might tell users that there is a problem in their account and they need to perform an urgent action or their

account will be suspended. Not surprisingly, Wang et al. (2009) found that the design of phishing emails always includes close attention to argument quality. What makes a phishing email successful is its high level of perceived acceptance by users. Users with a low level of perceived acceptance are more likely to suspect phishing emails. This difference in perceived level of acceptance reflects differences in individual characteristics. The level of acceptance of a phishing email can be increased through careful design. Wang et al. (2009) identify four key design features that are used to enhance the credibility of phishing emails (see Table 1).

Table 1: Key design features (Wang, Chen, Herath, & Rao, 2009)

Dimensions	No.	Features
Email title	3	Impact, Company name, Urgency
Email argument quality	7	Event, Impact, Urgent, Courtesy, Justification, Response action requested, Penalty
Message appearance	8	Authentic looking email sender, email signatory, Personalization, Media type, Typo, Third party icon for trustworthiness, Copyright, Company logo
Assurance mechanism	7	Third party icon for assurance, Anti-fraud/privacy statement, SSL padlock, General security lock, Help link/feedback, mechanisms, Authentication mechanisms, HTTPS link

- *Email title:* An attractive title increases users' motivation to open these emails. In psychology, motivation is defined as "an internal state or condition, sometimes described as a need, desire or want, that serves to energize behaviour and give it direction" (Kleinginna & Kleinginna, 1981). The main goal of a phishing email's title is to encourage users to open it.

- *Email argument quality (central route):* This refers to the strength of the argument embedded in a message (Bhattacherjee & Sanford, 2006). Argument quality increases the likelihood that the argument in a message will be accepted. In the ELM, this is known as a central route process of decision making. If users

accept the argument (e.g. that there is a problem in the system), they will agree with the message's conclusion and comply with the embedded action.

- *Message appearance (peripheral route):* Well-designed images and copyright information will increase message credibility. In the ELM, this is called a peripheral route of decision making (Petty & Cacioppo, 1986). It is assumed that victims of phishing emails fall because they are mainly judge message credibility using the peripheral route (Dhamija et al., 2006).

- *Assurance mechanisms:* Signs assuring the privacy or security of information increase users' trust and reduce any perceived potential risks, such as loss of money or private information (Lee & Rao, 2007). Grazioli (2004) suggests that users who base their judgment on assurance cues are at higher risk of becoming victims.

2.2.2 Persuasive techniques

Sharma (2010) studied 150 phishing emails randomly selected from 3181 such emails collected by the Anti-Phishing Working Group. A categorical content analysis and semantic network analysis were used to investigate how these emails persuaded users to perform the embedded action. Sharma identified three key dimensions: source credibility, message credibility and message structure.

Source credibility refers to those features that make the message appear trustworthy because it comes from a reputable organisation. Sharma measured six such indicators of source credibility (see Table 2): legitimate sender prefix (e.g. security, service), legitimate sender domain (e.g. ebay.com.au or nab.com.au), clear specific sender (e.g. IT department), contact telephone number, contact email address and company logo.

Table 2: Source credibility (Sharma, 2010)

Index	Frequency	Percentage
legitimate sender (prefix)	110	73%
legitimate sender domain	112	75%
clear specific sender	99	66%
Contact telephone number	5	3%
Contact email address	6	4%
company logos	67	45%

Message credibility refers to the effect of both the appeals contained in a message and its structure (Sharma, 2010). Sharma identified three categories of message appeals (rational, emotional and motivational) and three characteristics of message structure (explicit message, message order and message length). The results of his analysis are shown in Table 3 and Table 4.

Table 3: Message credibility (Sharma, 2010)

Index		Frequency	Percentage
Rational appeal	Reasoning from cause	116	77%
	Reasoning from sign	25	17%
	Reasoning from analogy	9	6%
Emotional appeal	Fear	92	61%
	Happy	5	3%
	Affection	40	27%
	None	13	9%
Motivation appeal	Safety	117	78%
	Belongingness/Love	14	9%
	Self-esteem	19	13%

In Table 3, *rational appeal* refers to the logic of the message argument. Rational appeals use formal logic rules as persuasive techniques. These techniques explain the relationship between two different events and take three forms:

- Reasoning from cause (event A is caused by event B).
- Reasoning from sign (event A is a sign of event B).
- Reasoning from analogy (events A and B are similar) (Dillard, 1994; Dillard & Pfau, 2002; Trenholm, 1989).

The importance of *rational appeals* in the design of phishing emails is supported by Wang et al. (2009). Phishing emails always present a justification (cause) for the response action (see Figure 4).

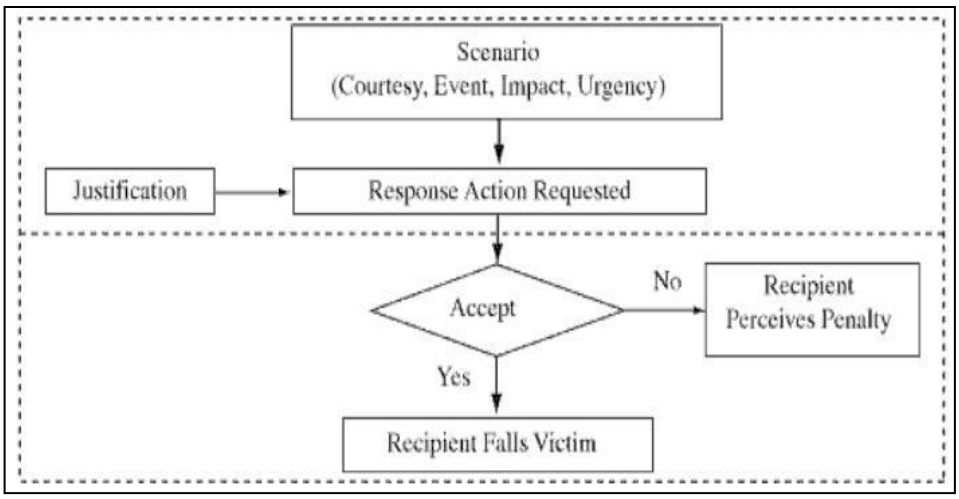

Figure 4: Argument quality measurement framework (Wang et al., 2009)

Emotional appeal refers to a message argument that targets users' emotions. Many phishing emails target negative emotions such as fear, distress and anxiety, and this has been found to increase the chances of users responding to these messages (Witte, 1992). For example, users may be told that they will incur a penalty if they do not comply.

Motivational appeal refers to a message argument that targets users' perceived needs (Gass & Seiter, 2007). According to Maslow's hierarchy of needs (Maslow, 1943, 1954, 1971), people are motivated to achieve certain needs (physiological, safety, belongingness/love, self-esteem and self-actualisation). When there is an apparent opportunity to satisfy these desires, they are motivated to act. Phishing emails exploit users' needs. For example, some phishing emails exploit users' need for safety by

suggesting that their account has been approached by an unauthorised entity, thus creating fear for the security of their information and money.

Message structure refers to the organisation of the message elements in a persuasive message. The main elements are shown in Table 4.

Table 4: Message structure (Sharma, 2010)

Index		Frequency	Percentage
Message	Explicit	136	90.67
	Implicit	14	9.33
Repetition	Repetition	50	33.33
	Non-repetition	100	66.67
Order	Climax	150	100

Explicit messages have been found to be more persuasive than implicit messages (Perloff, 2010; Trenholm, 1989). Repetition has a negative impact on users' attention and interest while moderate repetition has a positive impact on persuasion (Dillard & Pfau, 2002; Trenholm, 1989). When a strong argument appears at the beginning of a message, the order is one of anti-climax; when it comes at the end, the order is one of climax. A message is more persuasive when it has a strong argument regardless of the position of the argument (Gass & Seiter, 2007). Longer messages are more persuasive than shorter ones when they have strong argument quality (O'Keefe, 2002).

The following section discusses the main decision making processes that have been reported from research on phishing emails. These help to shed light on key areas of vulnerability among users.

2.3 Cognitive Processes in Decision-Making

This section explores the cognitive processes that users employ to judge phishing emails and account for their subsequent actions. This is important for identifying weaknesses in users' decision-making that lead them to respond to phishing emails.

We examined three main decision-making models: the model of detecting deception (MDD), the decision-making model and the elaboration likelihood model (ELM). These were chosen because they can help to identify areas of weakness in users' decision-making with regard to phishing emails.

2.3.1 The model of detecting deception (MDD)

The MDD applied the theory of deception in computer based environment (Grazioli, 2004). According to The theory of deception the detection is a cognitive process which involves examining different cues (e.g. words tone with body language) (Johnson & Grazioli, 1993; Johnson et al., 1992). The theory of deception is applied on a high rich medium (face-to-face). Face to face medium provides rich information which detectors can use to identify deception. Some of these richness's are: real time response, ability to examine different signs (e.g. vocal sign and body signs) and two path conversations between detector and deceiver. In a computer based environment, the process has one-way conversation. This means that in a computer based environment, the deceiver sends a message to the user and the user has to make a decision based on available information carried out by the message. One-way conversation is unlike in a face to face environment where a user can ask questions and observe real time response such as face or sound changes.

MDD divides the cognitive process of users' decision-making into four phases (see Figure 5). The first phase is *activation***,** which occurs when users encounter something different from what they are expecting. In the second phase, *hypothesis generation*, users try to develop an explanation for the identified difference between expectation and observation. To test the validity of these explanations, users enter the third phase, *hypothesis evaluation*, in which they employ different evaluation methods. For example, a user may suspect that an email asking for bank details is a phishing email and develops the hypothesis "legitimate email can be confirmed by its issuer". The user calls the bank to confirm the legitimacy of the email. In this case, the telephone is used to evaluate the hypothesis. *Hypothesis generation* and *hypothesis evaluation* both do not necessary need to be one time processes. A user can generate many hypotheses and evaluate them as much as he or she can. Finally,

the user will sum all the results from *hypothesis evaluation* and reach to the final phase. G*lobal assessment* is the final phase which the evaluated hypotheses are considered and a final decision is made about what action is to be taken in regard to the suspected email. More importantly, Grazioli conclude that commencing the model of detecting deception does not guarantee that users will always be detectors. Detectors and victims have gone through the four phases of the model of detecting deception. However, only detectors were able to detect deception, whereas victims failed to detect it (Grazioli, 2004).

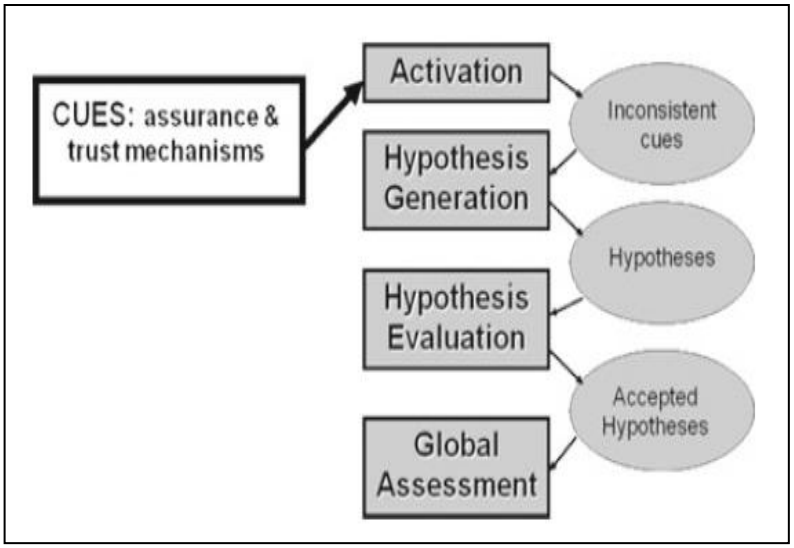

Figure 5: Model of detecting deception (Grazioli, 2004)

Wright et al. (2009) conducted a study in phishing emails and found two more important factors that are responsible for activating users' suspicion, which is the first phase in MDD. These factors are priming and individual factors (see Figure 7). Priming is defined as any experience that brings a cognitive structure to the mind that makes it available for employment in a subsequent mission (Higgins & Kruglanski, 1996). In other words, priming is a mechanism that warns users about possible deceptive behaviour, such as banks inform their clients that they will never ask about passwords via emails. Individual factors are those that differentiate users from each other. Wright et al. (2009) showed that users who have the same training and priming and are faced with the same phishing email have different responses. Some of these

users become detectors and others become victims of the phishing email. This means that there are individual factors of the users themselves that make some of them detectors and the other victims. These factors should be investigated and identified.

In our research, we applied MDD model to understand users' detection behaviour when they are faced with phishing emails. Based on MDD which is a cognitive process, we were able to extract three main phases in users' detection behaviour: susceptibility, confirmation and response (see Figure 9). For more details about these three phases please see Sections 3.2.4, 3.2.6, and 3.2.7.

Susceptibility is the first phase in users' detection behaviour. Users begin their detection behaviour by suspecting the phishing email. Based on the level of susceptibility, users will decide upon their intended behaviour (see Figure 9).

Confirmation is the second phase in users' detection behaviour. Users who become doubtful about a phishing email will choose a suitable channel to confirm or deny their doubts. For example, when questioning the legitimacy of an email, some users may contact organisations by phone, while others may email their friends.

Response is the last phase in users' detection behaviour. After users come to a decision about a suspected phishing email, they will choose the best way that they think to deal with suspected phishing email. Ultimately, users can be either detectors or victims. Victims are those who chose to perform the action in phishing emails. Detectors are those users who saw the phishing email and chose to ignore it.

2.3.2 The decision making model

The decision making model (Xun et al., (2008) was developed to explain users' cognitive process in relation to phishing emails (see Figure 6). The main feature of this model is its ability to identify two main areas of weakness in users' decision making: the type of selected cues and the interpretation of the selected cues. Users may select the wrong cues to judge the legitimacy of a phishing email. For example, they may assume that an email containing a logo is legitimate. In fact, phishing emails may contain simulated company logos to enhance their credibility. The second area of weakness is incorrect interpretation of cues that have the potential to

alert the user to the fact that this is a phishing email. For example, a user may (incorrectly) interpret an email request for private bank details as part of normal bank procedure. Similarly, some users have been found to misinterpret phishing email cues such as missing images (red Xs) as a system fault (Downs et al., 2006).

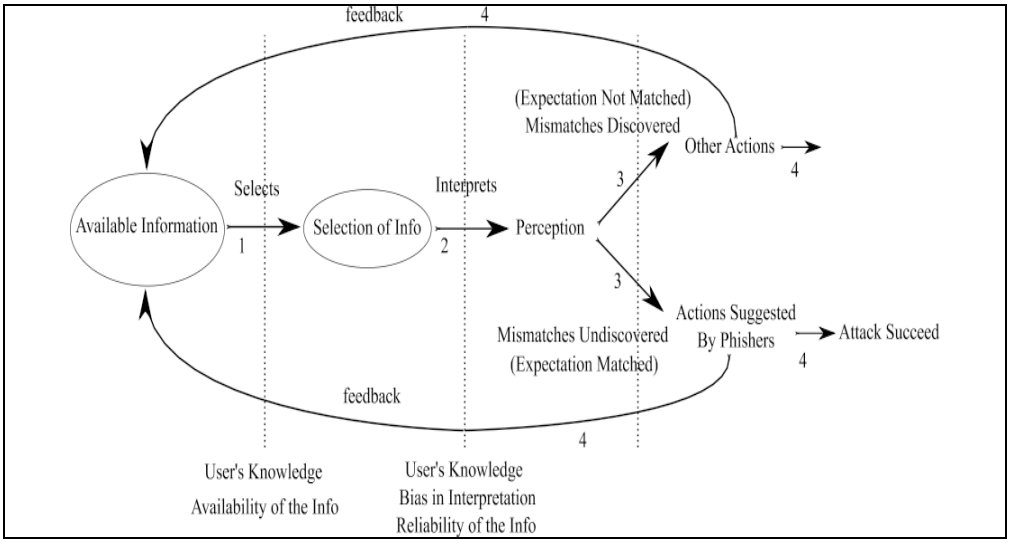

Figure 6: Decision making model (Xun et al., 2008)

2.3.3 The elaboration likelihood model (ELM)

The ELM proposes that users process message information via two main routes: the central route and the peripheral route (Petty & Cacioppo, 1986). The central route processes the message by examining the argument it contains and the benefits and costs of following the instructions (cognitive processing). The peripheral route processes the message according to its overall appearance or other features external to the argument it contains. It has been suggested that users who fall victim to phishing emails are those who use the peripheral route (Vishwanath et al., 2011). In the peripheral route, emails are judged by their appearance (e.g. images) and overall design. Aburrous et al. (2010) found that some users ignore phishing email cues and base their judgment on the attractive appearance (e.g. colours, animation and images). A recent study using the eye-tracker technique showed that users pay more attention to the content of phishing emails than to meta-data such as "From" email address (Pfeiffer, Theuerling, & Kauer, 2013). As previously explained

(Section 2.2), phishing emails are cleverly designed. Users who rely on the peripheral route to detect deception are particularly vulnerable.

These three models explain the cognitive process that underpins users' judgement of the legitimacy of phishing emails. Because the aim of the present study is to understand the phases in users' detection behaviour, the most appropriate model is the MDD. The main difference between MDD model and the other two models is its ability to explain the cognitive process outside the design features of phishing emails. The ELM and decision making model are explaining the cognitive process based on the design features of phishing emails. For example, ELM explains the detection based on the way that users examine phishing emails. There are two ways of judgment: overall looks or argument quality. Both of these ways do not help our research in identifying behaviour. The decision making model explains the detection by cues selection and cues interpretation. Again, decision making model depends on the design features of phishing emails. The following sections examine the differences between detectors and victims.

2.4 Cognitive Processes in Detectors and Victims

One way of identifying weaknesses in victims' detection behaviour is to compare their behaviour with that of detectors. To the best of our knowledge, no previous study has done this. Grazioli (2004), however, compared the cognitive process of detectors and victims. This is a useful foundation for better understanding the factors behind users' behaviour.

In Grazioli's (2004) study, participants were randomly assigned to one of two websites, a phishing website and a legitimate website. The findings suggest that there are significant differences between detectors and victims in two main cognitive phases—hypothesis evaluation and global assessment (see Table 5). Detectors use different cues to evaluate hypotheses and judge the authenticity of websites. The study did not seek to explain these findings (i.e. what makes detectors better at evaluating hypotheses or why they depend on different cues).

Table 5: Differences between detectors and victims (Grazioli, 2004)

MDD Phases	Detectors	Victims
Activation	Inconsistence cues	Inconsistence cues
Hypothesis generation	Priming[6] not significant	Priming is significant
Hypothesis evaluation	Competence at evaluation	Incapable of evaluation
Global assessment	Assurance cues	Trust cues

Wright et al. (2009) used Grazioli's MDD model to investigate the impact of individual user characteristics on detection behaviour. They interviewed detectors to identify the factors that helped them to detect phishing emails. Because the study did not include victims, no comparison was possible. Nonetheless, the study identified three influential factors in the first phase of the deception detection process (activation): cues, priming and individual factors (see Figure 7). Cues, or signifiers of phishing emails, have been well documented (Dhamija et al., 2006; Downs et al., 2006; Xun et al., 2008). Priming is defined as information stored in the memory that can be recalled at a later time (Higgins, 1996). In other words, priming can be used to warn users about possible deceptive behaviour. Priming has been found to increase sensitivity towards deception (McCornack & Levine, 1990). Cues and priming are well established in education and training materials. Individual factors have received less attention in the field of phishing emails. Our research aims to fill this knowledge gap by investigating the impact of users' characteristics on each phase of detection behaviour.

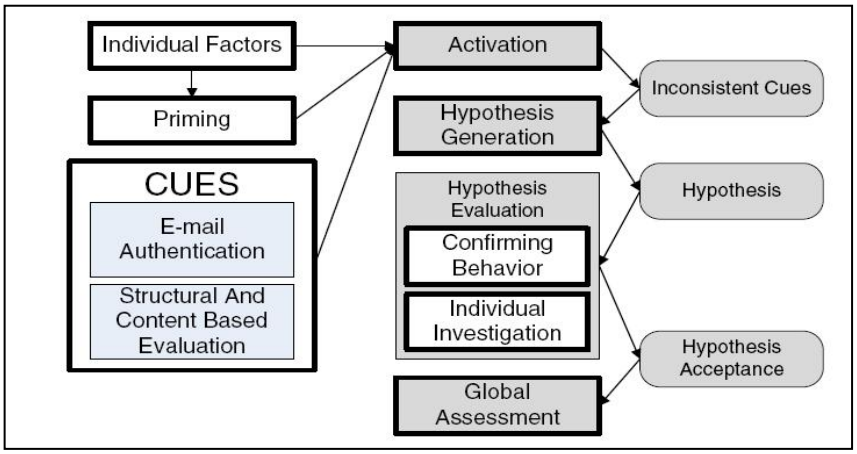

Figure 7: Updated model of MDD (Wright et al., 2009)

[6] Priming is a way of warning users about a deceptive behaviour.

Vishwanath et al. (2011) found that most users who fall victim to phishing emails use the peripheral route in their decision making (see Section 2.3.3). In other words, victims base their judgment on design features such as images and appearance. The study suggests that victims choose the peripheral route when they do not have enough time to process a large number of emails carefully. The study also found that knowledge and self-efficacy were associated with high elaboration in decision-making (central route) but elaboration did not prevent some users from being victims. Drawing on Grazioli's (2004) work, we can suggest that those victims may not generate a strong hypothesis or may weakly evaluate their suspicion.

Burns et al. (2011) propose that an important factor differentiating victims from detectors is their assumption that phishing emails will not target them (Davinson & Sillence, 2010). As a result, victims display a lower level of security behaviour in relation to checking the authenticity of emails in their inboxes. This assumption needs to change if users' behaviour is to change (Burns, Durcikova, & Jenkins, 2011). It is not enough merely to warn users about the dangerous effects of phishing emails; they also need to be educated in how to identify phishing email cues. Simply knowing that phishing emails can reach users will not improve their detection (Sven et al., 2007). Users expect to receive emails in their inbox and to respond to them. Therefore, users' detection ability should be improved in a way that does not affect how they deal with legitimate emails.

Since little is known about users' ability to detect phishing emails, the following discussion focuses on observed weaknesses in their ability to detect phishing websites, which employ similar deceptive techniques.

2.5 Users' Weaknesses in Identifying Deception Cues

Websites provide users with signs (indicators) that can be used to evaluate the authenticity of the site. These signs, known as browser security indicators, appear in browsers because the content of webpages can contain any kind of information and does not necessarily enforce security. Browser security indicators, however, are not sufficient for effective security (Dhamija & Tygar, 2005; Downs et al., 2006; Herzberg & Gbara, 2004; Mannan & van Oorschot, 2008). Users find it difficult to

confirm the authenticity of a visited website. Authentication can be revealed in various ways, such as a website security certificate, but there are usability issues associated with authenticating websites and security cues so that users can ensure that the information they are transferring over the Internet is encrypted (Mannan & Oorschot, 2008). These forms of insurance can be identified through padlock icons in browsers and "https" in URLs (Kuo, 2008). The factors responsible for security lapses are explored in the following sections.

2.5.1 Checking indicators

Browser security indicators are intended to help users assess the authenticity of visited websites (Downs et al., 2006) but only a minority of users rely on these indicators to make such judgments (Downs et al., 2006; Mannan & Oorschot, 2008). Mannan and van Oorschot (2008) found that 23% of users rely on the content of the webpage to authenticate the website while only 9% check all the browser security indicators for this purpose. Relying on content alone is inadequate because webpage content contains information chosen by the webpage designer. It has also been found that only 35% of users notice the existence of the "s" in the address bar (Downs et al., 2006) and that these users did not realise that the extra "s" indicated security.

2.5.2 Understanding indicators

Browser security indicators are deployed to deliver messages such as secure connection and server authentication (Dhamija et al., 2006; Downs et al., 2006; Mannan & Oorschot, 2008). Some users notice some indicators but often do not know what they mean (Downs et al., 2006). In fact, the majority of users do not know the real meaning of browser security indicators (Dhamija et al., 2006). For example, one security indicator is the padlock icon. Unlike the padlock icon in the browser chrome, a padlock icon in the content of the web page does not necessarily indicate an encrypted connection. Users usually do not know the difference and do not realise that a webpage can contain any icon that a web page designer wants to include (Mannan & Oorschot, 2008).

2.5.3 Faked indicators

For the minority of users who check and understand all browser security indicators (Downs et al., 2006; Mannan & Oorschot, 2008), there remains a serious

problem—they can be faked (Adelsbach, Gajek, & Schwenk, 2005; Herzberg & Gbara, 2004; Li & Wu, 2003; Ye, Yuan, & Smith, 2002). Therefore, users who look for security indicators can still be tricked into connecting to a malicious server. This can be achieved by redirecting victims to a malicious website that displays similar signs to those on the legitimate one (Juels, Jakobsson, & Stamm, 2007; Karlof, Shankar, Tygar, & Wagner, 2007a; Wu, Yao, & Bao, 2008). For example, a self-signed certificate can display the "s" in the Uniform Resource Locator (URL) to encrypt information transferred between the victim and the malicious server (Mannan & Oorschot, 2008).

An attacker can also create a spoofed image without implementing its real purpose (Dhamija et al., 2006; Ye et al., 2002); for example, showing a padlock icon in a spoofed window where there is no secure connection (Ye et al., 2002). Even careful users who check indicators can be tricked by advanced phishing attacks. According to Karlof et al. (2007), attackers can present the exact URL requested by users when they are actually connected to the malicious website. In this form of attack, users type and request the correct URL but the domain name system (DNS), which is poisoned, will connect them to a malicious website. This is an example of an attack that uses advanced forms of trickery to lure users. Clearly, there are serious issues associated with browser security indicators.

In summary, there are weaknesses in users' ability to identify phishing websites. These vulnerabilities should apply equally to phishing emails, which employ similar deceptive tactics. Various solutions to this problem have been developed, but users still fall victim to phishing emails. The following section discusses and evaluates these solutions.

2.6 Protective Strategies

This section provides an overview of the array of defences that have been designed to address the problem of phishing email attacks (see Figure 8). These falls into two main categories: strategies to prevent phishing emails from deceiving users, and techniques to protect users' accounts.

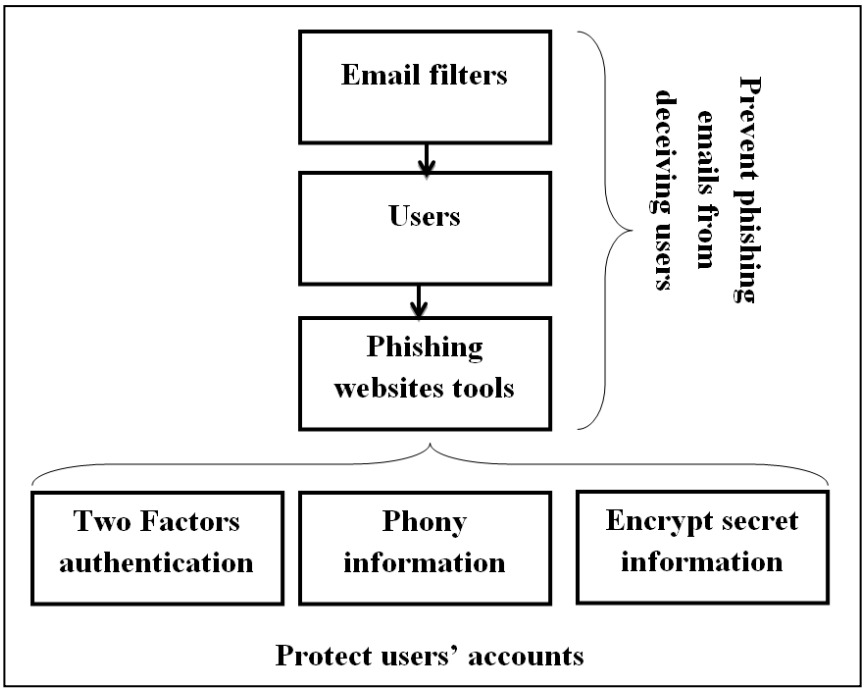

Figure 8: Forms of protection against phishing emails

2.6.1 Preventing phishing emails from deceiving users

The first defence against phishing emails reaching a user's inbox is the email filter (Bergholz et al., 2010; Fette et al., 2007; Maldonado & L'Huillier, 2013). The second form of defence involves users themselves, and the third comprises phishing website tools that are designed to prevent users from entering their secret information on phishing websites.

2.6.1.1 Email filters

Email filters are generally the first line of defence against phishing email attacks. They are intended to prevent these emails from reaching the user's inbox. Different approaches have been used. For example, an organisation may employ 30 analysts to prevent phishing emails from reaching users in the organisation (Knight, 2005). As well as manual authentication, some solutions rely on advanced technology. Phishing email filters can be divided into two main types: those which automatically delete identified phishing emails without user involvement, and those which issue a warning to users and leave the final decision to users themselves.

The first type is designed to detect phishing emails before they reach the user's inbox (Murphy, 2005). Different techniques of detection are employed. For example, Chandrasekaran et al. (2006) used distinct structural features to identify phishing emails. Fette et al. (2007) developed a machine learning system based on ten features of phishing emails that can be adapted to recognise newly developed features. Additionally, it has been proposed that digital email signatures improve detection ability (Garfinkel, Margrave, Schiller, Nordlander, & Miller, 2005).

The second type is designed to warn users about phishing emails. This type of filter cannot detect all forms of phishing emails (Fette et al., 2007; Maldonado & L'Huillier, 2013). Even if it could, the final decision is made by users, who may choose to ignore the warning.

Neither of these email filters can detect all types of phishing emails (Chandrasekaran et al., 2006; Cook et al., 2009; Fette et al., 2007; Maldonado & L'Huillier, 2013). This is because they mainly detect phishing emails from their design, which does not remain constant over time (Wang et al., 2009) or known to email filters developers. These email filters, therefore, must continually be updated.

An addition complexity can be added to email filters by considering new designed phishing emails. There is usually a time delay between an update and the creation of a new phishing email (zero-day). According to Kumaraguru (2009), users' response time to a phishing email is between two and eight hours after the phishing email was sent. Therefore, anti-phishing filters that depend on a black list have to be updated regularly, with this time frame in mind, or they will not detect new phishing emails (zero-day). It is up to users to determine the legitimacy of phishing emails that are not detected by filters.

Out-of-date email filters and undetected phishing emails mean that users have to rely on themselves to detect these emails. Their decision will determine whether or not they become victims. The following section describes solutions that have been developed to help users reach the right decision.

2.6.1.2 Educating users

Since users are the main target of phishing emails, high priority should be given to increasing their protection. Users may fall victim to phishing emails simply by opening them. Phishing emails may contain links to malicious downloadable files that destroy users' computers. Improving the ability of users to detect phishing emails, therefore, is a critical consideration and various educational programs have been developed for this purpose

Educational programs have shown promising results in improving users' detection ability (Alnajim, 2009). Existing programs, however, fail to take into account differences between detectors and victims. Studies have shown, for instance, that some users manage to detect phishing emails without any training. These users have received less research attention because previous studies have mainly focused on improving the success of educational programs around detection (Bekkering et al., 2009; Kumaraguru et al., 2008; Sven et al., 2007).

Such programs have not, however, solved the problem, since many users fall victim to phishing emails despite receiving education (Karakasiliotis et al., 2006; Kumaraguru et al., 2009). Clearly, other factors affect users' vulnerability. Identifying these factors is one objective of the present study. Its focus, moreover, is on users themselves, whereas educational programs focus on the technical aspects of protection against phishing emails.

In summary, users show some ability to detect phishing emails but not all can do so. These users continue to be harmed because they provide their confidential information or become connected to a phishing website. The following subsection discusses the solutions that have been developed to tackle phishing websites.

2.6.1.3 Phishing website security tools

Phishing websites are most commonly the next step in a phishing email attack. Another form of protection, then, targets these sites themselves. There are two main types of security tools for phishing websites: (1) those that help users to detect phishing websites and (2) those that exclude users from the decision-making process.

Firstly, detection tools use information from websites to improve the detection capability of browsers (Dhamija & Tygar, 2005; Herzberg & Gbara, 2004; Oppliger et al., 2006; Xia & Brustoloni, 2005) and the ability of users to authenticate websites (Dhamija & Tygar, 2005; Herzberg & Gbara, 2004; Li & Wu, 2003; Wu, Miller, & Little, 2006; Xia & Brustoloni, 2005). Giving users the right tools allows them to view some security features on websites. Four examples are discussed below: warning windows, website logos, dynamic security skins and personalising windows.

Warning windows tell users whether their connection to a website is secure or not (Xia & Brustoloni, 2005). This is achieved through the use of self-signed certificate warning windows. Unfortunately, it has been shown that more users choose to proceed with the connection than choose to stop when one of these windows appears (Whitten, 2004).

Website logos are used to authenticate legitimate websites via a tool known as a Trusted Credentials Area (TCA) (Herzberg & Gbara, 2004). Users are presented with an authenticated website logo rather than a URL. This approach facilitates authentication by users, since authenticating URLs is not an easy task. A difficulty with this approach is that authenticating a website's logo is based on its certificate, which exposes the validation process to SSL certificate problems (Dhamija & Tygar, 2005).

Dynamic security skins (DSS) are designed to generate a unique image for websites which appears in two places: in the background of the web page and in a trusted window from the legitimate server (Dhamija & Tygar, 2005). Users then have to visually match the two images to authenticate the server. Users, however, have to reveal their username before DSS authentication takes place and it is easy for a phishing attacker to catch the username (Wu et al., 2008).

Personalised websites have been proposed as a way for users to authenticate legitimate websites. This toolbar personalises concepts in an adaptive web browser, allowing users to access basic information at a glance (Adelsbach et al., 2005). It is claimed that this toolbar is able to defend against attacks that use active web languages, since it is located locally in the user's machine. This approach has two

main drawbacks: users have to recognise their personal image at every login (Wu et al., 2008), and toolbars can be spoofed (Wu et al., 2006).

These security tools leave the final decision to users. They enhance decision-making by providing users with technical means of authenticating websites and applying security measures. Even when such toolbars achieve a high rate of success in distinguishing between phishing and non-phishing websites, they have two main limitations: users may ignore the warnings and, if the solutions fail, users are not prevented from providing their secret information (Egelman, Cranor, & Hong, 2008; Wu, Miller, & Garfinkel, 2006).

Secondly, the other kinds of tools have been designed to provide protection by excluding users from the process of revealing their secret information to websites. This is because users can be tricked into authenticating malicious websites (Karlof et al., 2007a; Karlof, Shankar, Tygar, & Wagner, 2007b; Wu et al., 2008). In this approach, users give their secret information to security tools which are able to authenticate legitimate websites. These tools then provide legitimate websites with users' secret information. Examples of this approach are described below.

Locked and encrypted cookies (Karlof et al., 2007; Wu et al., 2008) protect users' credentials from being accessed by unauthorised parties by storing users' credentials in encrypted cookies. Encrypted information cannot be retrieved by websites that do not have access to the relevant decryption information. This approach has two main advantages. First, users' credentials are better protected by encryption. Second, only the website that encrypts these cookies has the ability to decrypt and obtain secret information. As with previously discussed strategies, however, cookies are not able to prevent users from revealing their credentials to phishing websites.

The active cookie scheme proposed by Juels et al. (2007) holds users' authentication and fixed IP address for servers. Protection is provided by changing the URL domain name to the server IP address. This addresses the attack tactic in which traffic from a legitimate server is redirected to a malicious one (Gupta, 2007). The disadvantage of presenting IP addresses, as shown in Downs et al.'s (2006) study, is that some suspect websites present an IP address instead of a URL. It is

clear to users that cookies are making the authentication, but this may have a negative effect in that users may refuse to deal with websites that present IP addresses.

Overall, cookies have three disadvantages: deleting cookies, obtaining cookies and authenticating browsers rather than users. One study found that nearly 58% of users delete their cookies at least once a month (O'Malley, 2005). In order to obtain authentication cookies, users have to make the initial authentication, which brings us back to the first problem associated with users making the authentication (Karlof et al., 2007a). Cookies authenticate users' browsers, not users themselves (Juels et al., 2007), which means that anyone using the authenticated browser can act on behalf of the authorised user.

In addition, malicious websites can manipulate these tools by pretending that the website is experiencing problems reading the information from the tools and asking users to enter their secret information manually. The tools cannot prevent this action. To address this issue, Wu et al (2006) designed a browser plug-in toolbar, called a web wallet toolbar, which prevents users from directly entering their secret information into online forms. The weaknesses in this solution are: 1) the toolbar does not prevent users from entering their web wallet information into a fake web wallet toolbar, and 2) not all users are willing to install the web wallet toolbar.

The solutions described in this section focus on the computer in preference to the user, because users may misinterpret technical security signs that can help them to avoid deception. In particular, users cannot distinguish between similar domains such as PayPal.com (with the letter L) and PayPa1.com (with the number 1), whereas computers can easily make this distinction. Users are required to create a strong password to protect their accounts. Because strong passwords can be hard to remember, users trade usability for security and choose an easy password (Cormac, 2009) and may use one password for many online accounts. This behaviour can result in users' passwords being leaked. For example, an adversary can ask users to create an online account to a free service and harvest the passwords.

The main drawback associated with these tools is their inability to prevent users from ignoring their warnings (Egelman et al., 2008; Wu, Miller, & Garfinkel,

2006). In addition, they require active user interaction, since their benefits will only accrue if users install them in the first place.

2.6.2 Protecting users' accounts

Some solutions are designed to protect users' accounts. They come into play if other solutions fail and users provide their secret information to phishing emails. In order to render captured information useless, some e-service providers use an account protection scheme such as two factors authentication, phony information, or information encryption.

The two factors scheme is based on identifying users by what they know and what they have, such as a token that contains a one-off password (Williamson, 2006). This approach ensures that the person requesting the e-service is the legitimate one. This is achieved by asking for information that is only available to the legitimate person (e.g. SMS message via mobile).

Phony information goes one step further by attacking the attackers. The attack begins by providing attackers with fake information and considering whoever subsequently uses this information as an attacker (Shujun & Schmitz, 2009). Not all e-service providers, however, apply these defences.

Encrypting secret information is a complicated approach that significantly increases the difficulty of obtaining secret information. For example, secret information can be stored in external hardware devices to prevent unauthorised access. Lin et al. (2007) developed a USB device that is able to encrypt and decrypt information outside users' computers. Rexha (2005) proposed a user certificate to protect the identity of the user. These certificates hold users' credentials encrypted by banks so that only banks that make the encryption can access users' information. These certificates allow users to make online purchases secure in the knowledge that their bank-related information can only be decrypted by the bank that issued the certificate. The main problem with these complicated solutions is the requirement for an external device. This device needs to be kept by the user and deployed for every transaction.

Despite all these available defences, users still fall victim to phishing emails. This suggests that both users and technology fail in some way. Moreover, not all e-service providers employ these devices. When technical solutions fail, users are the last line of defence against phishing emails. Yet users themselves have been neglected in research to date, which has largely focused on their detection ability in general. Clearly, there is a need to improve users' ability to detect phishing emails. To accomplish this, there is a need to identify users' vulnerabilities more specifically through better understanding how they deal with phishing emails and what factors affect their detection ability. This is the focus of the present study.

2.7 Gaps in Understanding Users' Detection Behaviour

There is a gap in the extant literature in relation to users' detection behaviour and the impact of users' characteristics on this behaviour. Differences between users have not been thoroughly investigated in the context of phishing emails.

Phishing emails include design features that make them credible. They mimic legitimate organisations to make users believe they originate from those organisations (Wang et al., 2009). Solutions have been designed to draw users' attention to phishing email cues such as digit IP addresses or unmatched URLs. Most security tools that are designed to detect phishing emails use these cues to achieve high detection accuracy (Chandrasekaran et al., 2006; Cook et al., 2009; Fette et al., 2007). While these tools have the ability to detect phishing emails and warn users about them, some users ignore these warnings because they are presented in a technical way that many users do not understand (Dhamija et al., 2006; Wu, Miller, & Garfinkel, 2006). Thus, usability is an important issue (Cormac, 2009).

Some users are able to detect certain types of phishing emails but can be tricked by other types (Jakobsson, 2007; Karakasiliotis et al., 2006). In other words, there is a relationship between the type of phishing email and users' detection behaviour. This suggests that users' ability to detect is the result of interaction between users themselves and the type of phishing email. For example, some users consider any email that requests financial information, such as bank account details,

to be a phishing email. These users may be tricked by phishing emails that ask users to update their account by, for instance, changing their password.

Some studies have reported the impact of users' demographics but fail to examine these findings more closely. For example, Kumaraguru et al. (2008) reported that, on day 28 of their experiment, there was no significant difference between the participants who had not received a single training session and those who had received multiple training sessions. They conducted the same experiment in a different culture and found a significant difference between trained and non-trained groups. This suggests that users' demographics, particularly cultural differences, play a major role in participants' ability to detect phishing emails. The researchers did not, however, compare the results of these two experiments.

Users also fall victim to phishing emails because they ignore warnings from security indicators and rely on themselves to evaluate certain cues in phishing emails, which does not ensure security (Stebila, 2010). This is another example of the impact of users' characteristics on their ability to detect phishing emails.

Users' awareness is another important factor (Aburrous et al., 2010). Current security indicators designed to warn users about phishing are not effective in preventing users from falling victim to these attacks. In other words, users need to be aware of how to detect phishing emails, not simply that they exist.

In summary, users' characteristics impact on their ability to detect phishing emails but these characteristics have not been thoroughly investigated in relation to their effect on detection behaviour and vulnerability. The following section discusses the variables that have been shown to affect users' detection ability, as well as others that are highly likely to do so.

2.8 Variables in Users' Detection Ability

This section discusses variables that have been examined or identified in general studies of deception as well as in research on phishing emails. Some variables that have been reported to affect users' ability to detect deception in general have not been investigated in relation to phishing emails. Other variables that appear

to affect users' ability to detect phishing emails have not been rigorously tested in research. In addition, some studies show contradictory results or used inappropriate measures. The present study addresses these limitations.

Users' characteristics are those factors which differentiate users from each other. Our research focused on those characteristics that make users vulnerable to phishing attacks and the impact of these factors on detection behaviour. This will help to identify potential victims, who can be targeted to increase their protection. The main characteristics that have been investigated are personality, culture and experience.

2.8.1 Culture

Although culture has not been directly investigated in phishing email studies, there are indications that it impacts on detection. For example, users from different cultures may not be able to identify spelling and grammatical mistakes in phishing emails (Jakobsson et al., 2007). Companies are no longer limited to their own geographic location and ecommerce companies increasingly target consumers worldwide. This means that customers come from cultures other than that of the company itself. What is the impact of an attack launched on a company that has customers from different cultures?

Phishing attacks are mainly based on emails. The fact that emails are a poor medium adds complexity to the problem of identifying phishing emails in a different culture. It has been shown that it is more difficult to detect deception across cultures when the deception is practised in a poor medium (Bond & Atoum, 2000; Bond et al., 1990). The problem is compounded because phishing emails can deceive even users who belong to the same culture as that of the impersonated company (Dhamija et al., 2006; Downs et al., 2006).

Cultural differences may play a major role in differentiating detectors and victims. Users from the same culture as that of the originator of a phishing email are likely to be more knowledgeable than others and, hence, better able to detect deception. For example, university students in a particular country may know that their university would never ask about passwords. Phishing emails which pretend to be from a university may have a high chance of tricking users from other cultures.

2.8.2 Personality

Two studies have highlighted the importance of personality in the ability to detect phishing emails.

The first study (Wright et al., 2009) was based on interviews with detectors of phishing emails. The findings showed a possible correlation between users' personalities and their success in detecting phishing emails. The personality variables identified in the study were: sensitivity towards the value of information; concern for privacy/security; obedience to instructions/authorities; and the Big-Five personality domains. Each is discussed in more detail below.

Users who suspected the phishing email showed high sensitivity when they were asked to reveal their SSC and showed a high level of concern about their privacy when asked to do so (Wright et al., 2009). Studies in ecommerce have investigated whether a high level of concern about privacy can be translated into secure behaviour. It was found that users showed high levels of concern about providing direct information but this did not stop them giving their information when presented with short-term benefits (Acquisti & Grossklags, 2005). Concerns about privacy may increase users' suspicions, which may lead them to activate the MDD. Such concerns do not, however, mean that users will detect phishing attacks.

Obedience may have an effect on the likelihood of users' becoming detectors. Users who detected phishing emails remembered that they had been instructed several times not to disclose their SSC to anyone (Wright et al., 2009). Because they had been repeatedly told to keep this information secret, they did not to respond to the email that asked them to reveal it.

The Big Five personality dimensions are: openness, conscientiousness, extraversion, agreeableness, and neuroticism. Each factor includes a cluster of characteristics that together make up one's personality. Wright et al. (2009) found that detectors score more highly on conscientiousness than victims. The analysis, however, did not include all detectors; detectors who did not inform a third party were excluded.

The second study (Kumaraguru et al., 2007b) used the Cognitive Reflection Test (CRT). Participants with a high CRT score were more likely to click on links from phishing emails that claimed to come from companies in which they did not hold an account. Users with high CRT are more vulnerable to visual illusions (Jensen, 1998). Phishing emails are deceiving users by implementing different techniques to make users believe their legitimacy such as including logos and padlocks.

2.8.3 Other variables have been identified in research on phishing emails

Several different variables have been suggested or investigated in previous studies related to users' ability to detect phishing emails. These are discussed below and summarised in Table 6. These variables are: age, gender, education, Internet usage and experience, email experience and knowledge about phishing emails which are discussed below.

Age has an effect on the ability to detect phishing emails (Kumaraguru et al., 2009; Sheng et al., 2010). Other studies, however, found that age does not have a significant effect (Dhamija et al., 2006; Kumaraguru et al., 2007; Sheng et al., 2007). The difference between these two groups of study is the division of age. These two sets of studies used different age categories, and this may have affected the results. Users aged 18 - 25 years behave significantly differently from older users, perhaps because they are more likely to be risk-takers.

Studies in gender suggest that there is a relationship between gender and users' ability to detect phishing emails, with females being more vulnerable than males (Jagatic et al., 2007; Sheng et al., 2010). This may reflect the fact that women are more likely than men to display agreeableness, and this may affect their vulnerability (Costa Jr, Terracciano, & McCrae, 2001).

Users' level of education has not been found to be a significant differentiating factor in their vulnerability to phishing emails (Dhamija et al., 2006; Sheng et al., 2007). Providing users with educational materials about phishing emails, however, increased their ability to detect phishing emails (Bekkering et al., 2009; Kumaraguru et al., 2009; Kumaraguru et al., 2008). Not all such educational materials are effective in increasing users' detection ability. One pre/post-test study, for example,

showed that the educational materials given to participants increased their fear of phishing emails and led them to rank non-phishing emails as phishing emails (Sven et al., 2007).

The number of years of Internet use was not significantly associated with differences in the ability to detect phishing emails (Dhamija et al., 2006; Sheng et al., 2007). Internet usage varies between users, who can employ it to communicate with friends or read newspapers, as well as for shopping or banking, which require security. The experience of conducting sensitive transactions on the Internet influences users' perceptions and behaviour. Those users who shop online are significantly more likely to detect phishing emails (Wright et al., 2009). This may be because shopping online requires users to pay attention to security and increases their experience of detection. In contrast, Kumaraguru et al. (2007) found that online shopping does not significantly differentiate detectors from victims.

Email experience has not been satisfactorily measured. Some studies (Kumaraguru, 2007; Kumaraguru et al., 2007) have not found any significant relationship between email experience and users' ability to detect phishing emails. These studies, however, asked about the number of emails that users receive in their email account. Users may use emails frequently, but this does not mean that they know how to evaluate them. Users may know how to send and receive emails, but they do not necessarily know that email addresses can be spoofed, or that a lock icon in the content of the email does not guarantee security. In contrast, Vishwanath et al. (2011) found that the number of emails received increased the likelihood that users would make decisions based on the appearance of the email, which increases their vulnerability to phishing emails.

Knowledge of the existence of phishing emails did not have any significant effect on users' detection ability (Wright et al., 2009). Knowing that security threats exist does not prevent users from becoming victims. Many users believe that the perpetrators of phishing emails are not interested in targeting them in order to steal their information (Herzberg, 2009). Education programs that seek to inform users about phishing email cues, such as IP addresses, have achieved some success in increasing users' detection ability.

Table 6: Summary of variables

Factors	Sub-factors	Relation with phishing detection	Findings
Culture		Significant	Non-phishing email studies
	Language	N/A	Spelling mistakes
	Nationality	N/A	
Personality	Sensitivity towards requested information	N/A	Qualitative results
	Concern about privacy/security	N/A	Qualitative results
	Big-Five personality dimensions	Significant	Detectors only
Age		Significant	Younger users
Gender		Contradictory[7]	Females
Education		Not significant	
Internet experience	Number of years	Not significant	
	Shopping	Contradictory	
Email experience	Number of emails	Contradictory	
Knowledge of phishing emails	Existence	Not significant	
	Cues	Significant	

2.9 Summary

This study emphasises the importance of including users in the process of detecting phishing emails. The problem of phishing emails has two dimensions—users and technology. Many technological solutions have been developed to tackle this problem, but few have approached it from the perspective of users. Most of the technical solutions are preventive and do not stop users from falling victim (Purkait, 2012; Yue & Wang, 2008). Users must remain alert to the threat from phishing emails and cannot always rely on currently available solutions to protect them. Dependence on these solutions can have a negative impact by encouraging users to

[7] i.e. some studies show a significant effect for the factor and others do not.

trust all the emails that arrive in their inbox. Yet the perpetrators of phishing emails are constantly finding new ways to overcome technical solutions (Wang et al., 2009). When phishing emails pass security tools, the chance of users becoming victims increases significantly.

Improving users' ability to detect phishing emails will help to reduce the number of victims. In many cases, users are the last line of defence against phishing emails. The present study is motivated by the need to find new ways to improve users' defences. Solutions that can detect phishing emails or prevent them from reaching users will facilitate this task. This is not always the case, however, and it is dangerous for users to rely completely on technological solutions. If they do so, they become easy targets.

We need to better understand users themselves in order to increase their protection. Specifically, it is vital to identify weaknesses in users' detection behaviour. Neither users' detection behaviour nor the impact of users' characteristics on this behaviour has been well investigated. Identifying those factors that make users vulnerable to phishing attacks is an important goal if their effects are to be reduced. At the same time, identifying those factors that are responsible for turning users into detectors will enhance efforts to address the corresponding deficiencies in victims.

Chapter 3: Research Model

This chapter explains how the research model was developed. Users' detection behaviour is examined from a theoretical perspective and user attributes likely to impact on that behaviour are identified. The research model and hypotheses are presented.

3.1 Model Building

As discussed in Chapter 2, despite the availability of many technical solutions and educational programs, users continue to fall victim to phishing emails (Wu, Miller, & Garfinkel, 2006). Educational programs are designed to increase users' awareness of the technical aspects of phishing emails but little research attention has been devoted to better understanding users themselves. Significantly, some educational program studies have observed demographic differences in users' detection ability but have not investigated these differences further. Clearly, there needs to be a greater research focus on the users' perspective. Before discussing users, the main theory used in our research is explained below.

The theory of deception is the main theory and defines the intended deception as a cognitive process between the deceiver (sender) and the deceivee (receiver) under conflict of interest (Johnson & Grazioli, 1993; Johnson et al., 2001; Johnson et al., 1992). The deceiver encourages the receiver to take a desired action by manipulating the environment of the receiver to produce an incorrect cognitive representation. This theory was originally developed to explain deception in information-intensive environments such as face-to-face conversations (Grazioli & Wang, 2001). Face-to-face interaction is considered to be a rich medium that can carry various cues to assist detection of deception. These include real time response, the ability to examine different signs (e.g. vocal and body signs) and two-way dialogue between detector and deceiver.

Grazioli (2004) applied the theory of deception in a computer based environment and proposed the MDD (see Figure 5). In this kind of environment, the

process mainly involves one-way conversation in which the deceiver sends a message and the user has to make a decision based on the information contained in the message. This environment makes detection more difficult compared to a rich medium like face-to-face interaction, where a user can ask questions and observe the response in real time. The process of detection in relation to phishing emails is explained below.

Users who open a phishing email fall into one of two categories: detectors or victims. Detectors are those who decide not to respond while victims are those who perform the requested action. Detectors and victims behave differently in reaching their respective conclusions (see Figure 9). The MDD allows us to investigate their behaviour from the beginning and to identify three main behavioural phases in detection: susceptibility, confirmation, and response. In the following, we will discuss our research hypotheses and the relationships between users' characteristics with users' behaviour with phishing emails.

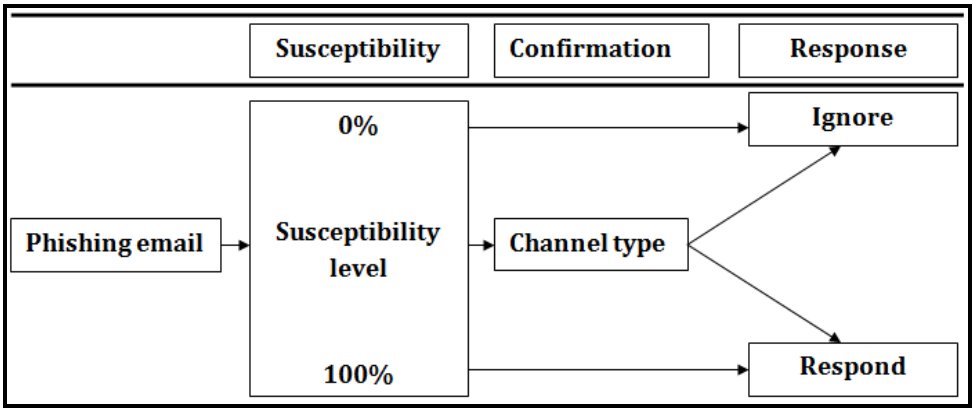

Figure 9: Users' behaviour when faced with a phishing email

3.2 Research Hypotheses

The research model that was developed and empirically tested in the present study is shown in Figure 10. Data were collected using survey, experimental and interview methods to obtain a holistic understanding of users' detection behaviour. In a mixed methods approach, the techniques complement each other and each has a specific purpose in relation to understanding the research problem (Gable, 1994).

Surveys were used to collect information about users' characteristics and evaluation methods. The experimental method captured the real-life behaviour of users when they encountered phishing emails and was used to categorise them as detectors or victims. Interviews generated in-depth understanding of users' detection behaviour. Research hypothesis were developed to illustrate relationships between variables.

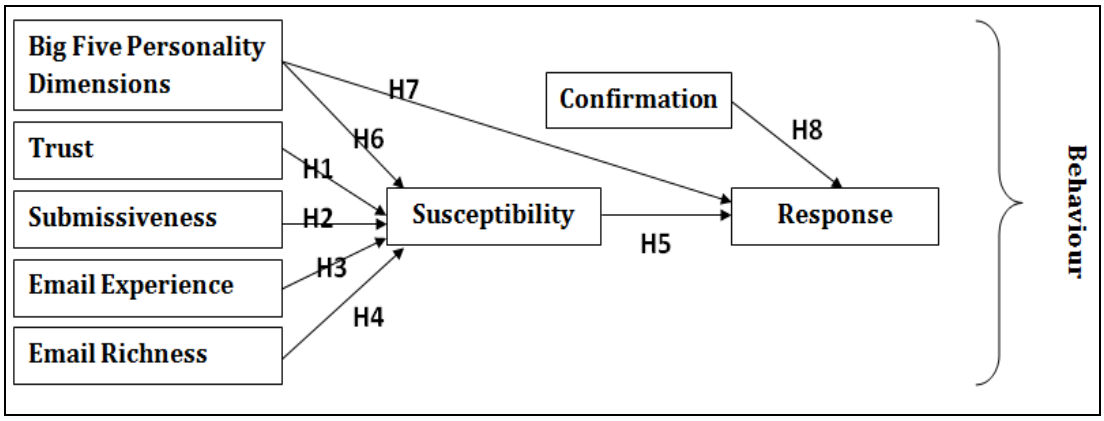

Figure 10. Research model and hypotheses

The research hypotheses in our study are as follows (see Table 8):

3.2.1 Trust

Trust is "to willingly become vulnerable to the trustee (another person, institution, or people generally) having taken into consideration the characteristics of the trustee" (Rousseau, Sitkin, Burt, & Camerer, 1998).

Trusts can be divided into two types: (1) Trust as a personal characteristic, which measures the trusting nature of a person. It measures a person's inclination to trust someone or some organisations, the trustworthiness of which the person has no prior knowledge of. (2) Trust as confidence of reliability in specific persons or organisations. This measures the trust that a person developed over time after he/she has dealt with the specific persons or organisations over time. As our research focuses on the user characteristics, our measure of trust focuses on the former.

H1: Trust increases users' *susceptibility* to phishing emails

Trust is measured with 3 items developed by McKnight et al. (2003).

3.2.2 Submissiveness

Submissiveness, or submission to more dominant entities (Allan & Gilbert, 1997), is associated with obedience and compliance.

Phishing emails are always request users to make an action in order to be successful. Submissiveness may increase the chance of users comply with phishing emails request. Users who have high submissiveness are more likely will not question the legitimacy of entities. In phishing emails detection, suspecting the legitimacy of phishing emails is an essential aspect to switch user to detection mode. Submissiveness has a negative impact on suspicion. Users who have high submissiveness are more expected to fall prey to phishing emails since they are more likely will not suspect. Furthermore, the qualitative findings of Wright et al. (2009) indicate that users who are submissive are more likely than others to submit with the requests of phishing emails.

H2: Submissiveness increases users' *susceptibility* to phishing emails

Submissiveness is measured with 16 items developed by Allan and Gillbert (1997).

3.2.3 Perceived email experience and richness

Perceived email experience is defined as users' ability to encode and decode information included in emails (Carlson & Zmud, 1999).

Perceived email richness is defined as users' ability to extract rich information contained in emails (Carlson & Zmud, 1999). Media richness is defined as the ability of the medium to convey rich information in its messages (Daft & Lengel, 1986).

Email, which is the main channel used for deception in phishing attacks, is a poor medium for the transfer of information and cues (Daft & Lengel, 1986). A poor medium (low information, few cues) makes the task of detecting deception via email very difficult for receivers (George & Carlson, 1999). Users find it hard to detect cues about the identity of phishing emails, yet cues are very important aides to detection (Downs et al., 2006; Grazioli, 2004; Xun et al., 2008).

Media richness theory uses four criteria to determine the richness of a medium: immediate feedback, multiple cues, language variety and personal emotions (Daft & Lengel, 1986). A medium in which all these features are present is considered to be a rich medium. The fewer the number of features, the poorer the medium will be. For example, face-to-face interaction is considered to be a rich medium because it meets all these criteria. Emails are viewed as a poor medium because they cannot meet all these criteria. However, email can be considered as a rich channel using channel expansion theory (Carlson & Zmud, 1999).

Channel expansion theory adds another dimension to the idea of media richness. Carlson and Zmud (1999) found that emails, which are a poor channel, can be perceived by users as a rich channel depending on their previous experience and the perceived richness of the email. Richness gives users a baseline for comparison between previously obtained information and information extracted from phishing emails. Comparison is viewed as the trigger for users' detection process.

In addition, some studies have examined the impact of users' experience with emails on their detection ability. The variable considered was the number of received emails. For example, Vishwanath et al. (2011) found a positive relationship between the number of emails received and users' vulnerability to phishing email attacks. They explain this result by suggesting that receipt of a large number of emails leads users to adopt the peripheral route in decision making. In other words, they judge the authenticated an email from its appearance which, as previously explained, is a risky approach (Jakobsson et al., 2007). This means that the stress associated with having to make a quick decision reduces the chances that they will make the right decision. Phishing emails exploit this by emphasising the urgency of the situation and pushing users to make a decision in a short time.

The number of emails received, however, is not necessarily an appropriate measure of users' experience with emails. Users may receive a high number of emails but not interact with them. In the present study, channel expansion theory is used to explain the relationship between email experience and ability to detect.

Perceived email richness measures users' ability to observe diverse cues in emails (Carlson & Zmud, 1999). A rich medium can contain a number of different

cues (Daft & Lengel, 1986). Emails can be perceived as a rich medium by users if they are able to extract diverse cues from them. Being able to observe different cues as to the identity of the sender of an email enhances users' ability to detect deception. Phishing emails are well designed to hide such cues. In order to spot phishing email cues, users need to pay close attention to specific details they contain and know what the cues mean. Failure to recognise these cues is the second source of error in users' detection decisions (Xun et al., 2008).

H3: Perceived email experience decreases users' *susceptibility* to phishing emails
H4: Perceived email richness decreases users' *susceptibility* to phishing emails

Our research proposes that email experience and richness have impacts on the ability of users to detect deception carried via emails. The measure includes 6 items for email experience and 4 items for email richness developed by Carlson and Zmud (1999). Please refer to Appendix A question number 14 for details.

3.2.4 Susceptibility

Susceptibility refers to the inability of users to suspect a phishing email. Users with a high level of susceptibility have low or no suspicion, and vice versa. Susceptibility comes into play when users open a phishing email to decide whether it is legitimate or not.

According to the MDD, users go through four cognitive phases to reach their final decision (see Figure 5). The first phase is activation, in which users suspect that the received email is a phishing email. The activation phase is triggered by inconsistency between observed cues and expected cues (Buller & Burgoon, 1996). Observation of cues cannot occur without the user opening the email. Therefore, the first behavioural phase in the detection process occurs when users open the phishing email. In the present study, this phase is called susceptibility, which is driven by users' level of suspicion towards phishing emails. Users with either low or high susceptibility will proceed directly to the third phase, response. Users with neither low nor high susceptibility proceed to the second phase, confirmation (see Figure 9).

According to Stiff et al. (1992), suspicion causes users to focus on making reliable judgments based on situational characteristics. Suspicion, then, reduces users' susceptibility to phishing emails, which employ techniques (such as

impersonating reputable organisations) to allay suspicion. As noted above, such techniques can lead to users exercising less care in authenticating emails.

Noticing phishing email cues leads detectors to perform the first step in the MDD, namely, activation. However, not all users are able to detect these cues. According to Xun et al. (2008), the first mistake victims make is mis-selecting cues. Some users select cues that have no relation to the task of detecting phishing emails (e.g. logos or padlocks). They fail to pay attention to important cues and remain unaware of the deception. Selecting the right cues differentiates detectors from victims.

H5: High *susceptibility* to phishing emails increases users' *response* to phishing emails

Susceptibility is the first phase in users' detection behaviour. Based on the level of susceptibility, users will determine their intended behaviour (see Figure 10). Therefore, we measured susceptibility with five phishing emails developed by the presented study (see Section 4.5.4).

3.2.5 Big five personality dimensions

The Big Five personality dimensions are: (1) extraversion, which describes a person who interacts more with others; (2) agreeableness, which describes a person who is more kind and warm to others and have good intentions; (3) conscientiousness, which describes a person who is more determined to complete tasks; (4) emotional stability, which describes a person who is more likely to be calm; and 5) openness, which describes a person who is more open to new experiences (Costa & McCrae, 1992).

Big five personality dimensions divide individual personality into five main categories. Each one of these category summarise more traits which can form the high level traits in these personality dimensions (Gosling, Rentfrow, & Swann, 2003). These personality dimensions have an impact on users' behaviour with people and entities. For example, a person who has high score in openness is keen to involve in new experience. In other word, openness could increase users to be more risk-takers or adventurers. Agreeableness involves believing in others and be less

suspicious. It can be seen that each one of these personality dimensions are responsible in making users behave in a certain way.

Phishing emails are one of these entities which are impact by these dimensions. In fact, phishing emails may benefit from some of these personality dimensions. For example, designing a phishing email which presents a prize for risky behaviour may attract users who have high score in openness. Those users are more eager to be involved in risky behaviour. Furthermore, Phishing emails are well designed to minimise users' suspicions. Would users who have high score in agreeableness be more victimised than other users. Since, agreeableness increase users' tendency to give good intentions to others. It has been argued in the current literature that the Big Five personality dimensions influence users' susceptibility to phishing emails (Parrish Jr, Bailey, & Courtney, 2009).

H6: Users with high scores on certain personality dimensions increase *susceptibility* to phishing emails

H7: Users with high scores on certain personality dimensions increase their *response* to phishing emails

The relationships between big five personality dimensions and users' susceptibility and response to phishing emails are measured in our research. The hypotheses for big five dimensions are: extraversion (H6a, H7a); agreeableness (H6b, H7b); conscientiousness (H6c, H7c); emotional stability (H6d, H7d); and openness (H6e, H7e). The measure used in the present study was developed by Gosling et al. (2003) and contains 10 items.

3.2.6 Confirmation

Confirmation channels are those channels which users choose to validate and evaluate suspected phishing emails.

Users who suspect a phishing email will choose a way to evaluate their suspicion. The confirmation phase is affected by the assumptions users make in their detection behaviour. Some users who are aware of phishing emails fall victim because they assume that no-one would be interested in targeting them (Burns et al., 2011; Davinson & Sillence, 2010; Dhamija et al., 2006). They either do not believe that they would receive a phishing email or that attackers would not be interested in

stealing their information. Users who make this assumption will not proceed to the confirmation phase (see Figure 9).

Confirmation behaviour plays an important role in detection. When users suspect a phishing email, they behave in different ways to verify emails legitimacy. Some of these behaviours are not appropriate. For example, some users who suspect a phishing email click on the embedded link on the assumption that, if a website similar to what they expect appears, the email is legitimate. This type of confirmation behaviour is not reliable, since phishing attacks are designed in a similar way. Wright et al. (2009) identified different types of evaluation such as forwarding, replying and asking others. Each of these behaviours can be performed through various channels.

Users choose the type of confirmation channel they think is appropriate. According to media richness theory, users will choose rich media when faced with uncertain tasks (Daft & Lengel, 1986). If users are uncertain about the task (e.g. whether to click on a link or reveal their password), they are more likely to choose a richer channel. For example, users will choose a rich channel such as face-to-face interaction. Users who are highly uncertain about an email request may choose phone or personal communication for confirmation. For certain tasks, users do not make much effort to evaluate the task using a richer channel but may even use a poor medium (such as email) for verification. Based on the result of this evaluation, they move on to the next step. The present study examines the impact of type of confirmation channel on users' detection behaviour.

Media richness theory can explain some aspects of users' behaviour that are related to the type of confirmation channel. For example, in Wright et al.'s (2009) study, participants had been repeatedly instructed not to give their super-secure code (SSC) to anyone, including their closest friend or lecturer. This instruction was reinforced by having participants sign a form stating that they would not disclose this information (SSC), and they received additional reminders from their lecturer. In the experiment, participants were sent an email request for their SSC. Some participants did not respond directly but waited for more robust information at the next lecture. These participants, in other words, chose a richer confirmation channel to resolve the uncertainty created by the contradiction between what they had been told (to maintain the secrecy of their SSC) and the request (to expose their SSC) in the email.

The contradictory requests came from two different channels that varied in terms of their richness, and this appears to have affected users' behaviour. The researchers did not examine this finding further, but our study will do so.

H8: Rich confirmation channel decreases users' *response* to phishing emails

In our research, we hypothesis that rich confirmation will reduce users being victim to phishing emails. In the present study, our interest was to investigate the relationship between the type of confirmation channel users choose and their response to phishing emails. This was measured by asking users to self-report the type of confirmation channel that they used. These confirmation channels are classified according to their richness (face to face, telephone, email or self-investigation). Face to face is considered to be a rich medium (Daft & Lengel, 1986).

3.2.7 Response

Response is the final action in users' detection behaviour. In the present study, response means that users have complied with the request embedded in the phishing email and have thereby become victims.

The final cognitive phase in the MDD is global assessment. In this phase, users sum up the results of their evaluation(s) and come to a conclusion. Some users rely on one strong hypothesis and its evaluation to reach a strong conclusion. Others rely on various weak hypotheses and outcomes. Grazioli (2004) found that detectors of phishing attacks rely on one strong hypothesis and examine different cues in the phishing email than victims. This suggests that detectors know what they are looking for. Both media richness theory and channel expansion theory (see Sections 03.2.3 and 3.2.6) are relevant to understanding why detectors examine different cues than victims. For example, victims rely on company logos or padlock signs and the overall look of the email to judge an email (Dhamija et al., 2006). While, detectors found to be using spelling mistakes as a vital sign for phishing emails (Downs et al., 2006). Based on the result of the global assessment phase, users choose to respond to or ignore the phishing email. In the present study, this behavioural phase is called response.

Table 7: Summary of constructs

Construct	Definition
Trust	Inclination to trust other people
Submissiveness	Submission to more dominant entities
Perceived email experience	Ability to encode and decode information included in emails
Perceived email richness	Ability to extract rich information contained in emails
Confirmation channels	Those channels which users choose to validate and evaluate their decision about suspected phishing emails
Susceptibility	Users' inability to suspect phishing emails
Big Five personality dimensions	The five main dimensions of personality
Response	Users' action in response to the phishing email used in our research

Table 8: Research hypotheses

Hypothesis	**Includes**	**Description**
H1	Trust	**Trust** increases users' *susceptibility* to phishing emails
H2	Submissiveness	**Submissiveness** increases users' *susceptibility* to phishing emails
H3	Perceived email experience	**Perceived email experience** decreases users' *susceptibility* to phishing emails
H4	Perceived email richness	**Perceived email richness** decreases users' *susceptibility* to phishing emails
H5	Susceptibility	High **susceptibility** to phishing emails increases users' *response* to phishing emails
H6	Extraversion, agreeableness, conscientiousness, emotional stability and openness	Certain types of **personality traits** increase users' *susceptibility* to phishing emails
H7	Extraversion, agreeableness, conscientiousness, emotional stability and openness	Certain types of **personality traits** increase users' *response* to phishing emails
H8	Confirmation	Rich **confirmation** channels decrease users' *response* to phishing emails

Table 8 List the hypotheses in our research in the “hypothesis” column. Some of the hypothesis includes several constructs under the main hypothesis which are explained in the “includes” column. For example, the hypothesis H6 and H7 are for big five personality traits which includes 5 constructs which form personality traits. The rest of the hypothesis H1, H2, H3, H4, H5 and H8 include one construct which are listed in the “includes” column.

3.3 Summary

This chapter has described the conceptual framework that underpins the design of the present study. It has explained the process used to identify users’ detection behaviour, defined the relevant parameters of the investigation and presented the research model and hypotheses.

Chapter 4: Methodology

This chapter explains how the theoretical framework developed in Chapter 3 was empirically tested. It describes the research design, participant selection and methods of data collection and analysis. Ethical considerations are discussed. The pilot study and the instruments used in the survey and experimental procedures are presented in detail. Some differences in the design of the Saudi Arabian and Australian studies are explained and justified.

4.1 Research Design

The study adopted an explanatory design using the participants' selection model (Creswell & Plano Clark, 2007). This model was chosen because the research focus is on two types of participants: detectors and victims (see Figure 11). The aim is to investigate the relationship between independent variables (users' characteristics) and dependent variables (*susceptibility* and *response* to phishing emails). Quantitative and qualitative methods of data collection and analysis were used to generate a comprehensive picture from a single study (Saunders, Lewis, & Thornhill, 2009).

A literature review was conducted to identify characteristics associated with users' ability to detect phishing emails and deception in general. An examination of relationships between variables was used to develop a conceptual model (see Figure 10). These steps have been explained in Chapter 3. This model was tested using a mixed methods approach comprising two surveys, a phishing email experiment, and interviews.

Before data collection commenced, a pilot study was used to test the survey instrument. After appropriate modifications had been made, the full study was implemented. The first survey was designed to collect data on users' characteristics and susceptibility. Next, we conducted an experiment in which phishing emails were sent to participants. This experiment enabled us to classify participants into detectors and victims. The second survey was then conducted to collect data on the evaluation

methods users employed after they received the phishing email. Finally, interviews provided deeper insight into users' detection behaviour. The methods used in our research are ordered as above and the time gap between them is around two weeks. In general, these methods should be done immediately one after another to gain accurate data. However, the time gap between these methods is not affecting collected data. Each method is specified for collecting different information. The first survey collects information about users' characteristics. The experiment which includes sending phishing email to participants does not relate to information collected in the first survey. The second survey informs participants about the real intention of our research which is phishing email study. Then, the second survey collects information about participants' behaviour with phishing email. Informing participants about our research intention needed to be delayed to avoid impacting participants who did not yet see the phishing email or decide what to do with the phishing email. Two weeks time was needed to give participants enough time to see and respond to the phishing email. Especially those participants who may ask other participants about the phishing email.

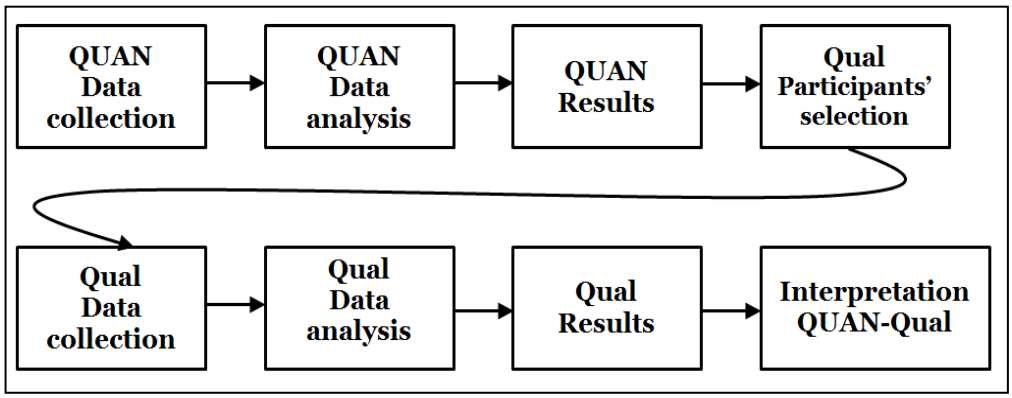

Figure 11: Mixed methods with participants' selection model

All data were analysed using appropriate software and tools. The results were validated and recommendations were made. The research plan is summarised in Figure 12.

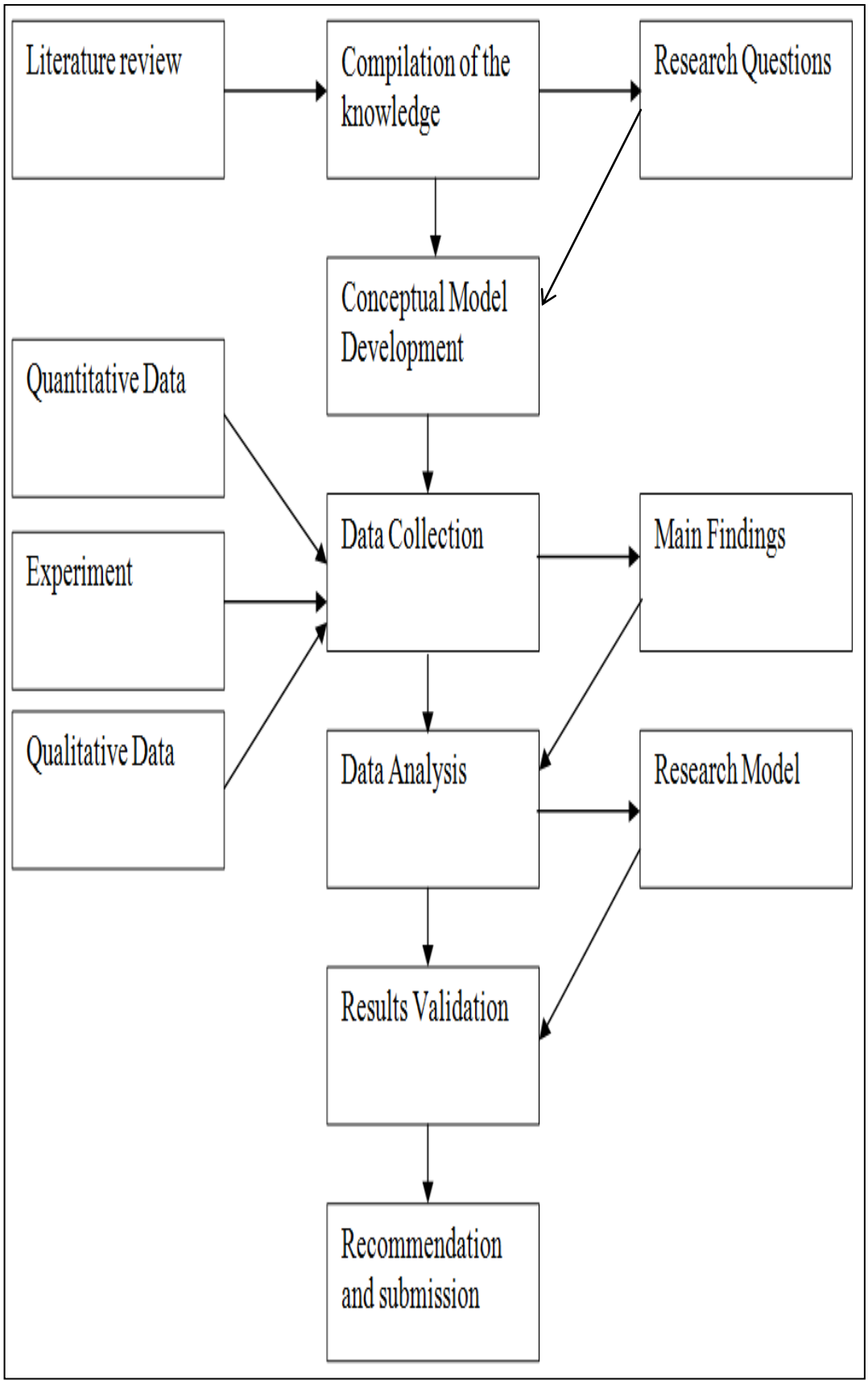

Figure 12: Research design

4.2 Participants Selection

The sample comprised undergraduate university students from two countries, Saudi Arabia and Australia. Undergraduate students were targeted because they have been identified as users who are most vulnerable to phishing emails (Kumaraguru et al., 2010; Sheng et al., 2010). Including elder users would have limited our ability to measure the impact of users' characteristics.

Convenience sampling "involves drawing samples that are both (1) easily accessible and (2) willing to participate in a study" (Teddlie & Yu, 2007). University students meet these criteria. The research design required that we be able to monitor and link participant data from three separate collection methods (survey, experiment and interview). In order to maintain anonymity, participants were assigned a number that was used to link their responses from each of these three data sources.

4.3 Data Collection

This section describes in detail each of the data collection methods that were employed in the study, namely, survey, experiment and interview.

Surveys provide an objective benchmark for research (Cavana, Sekaran, & Delahaye, 2001) and are the most efficient way of collecting quantitative data from large samples (Darlington & Scott, 2002). We used the survey method to collect data on users' characteristics (the independent variables) and measure the impact of these characteristics on the process of detecting phishing emails in two samples (Australia and Saudi Arabia).

In our research, we want to find the impact of users' characteristics on their ability to detect phishing emails. Survey was used to collect information about users' characteristics. Users, ability to detect phishing email can be done by knowing users response to phishing emails. The most suitable data can be obtained from real users who were encountered with phishing emails. However, obtaining this kind of information from organisations is not affordable, since it relates directly to users' privacy. Other way can be seen in some studies which used images of phishing

emails and ask participants to rate phishing emails legitimacy (Jakobsson et al., 2007; Sheng et al., 2010). Our research interested in capturing real behaviour of users with phishing emails. Showing images of phishing emails is measuring the intention of users not the actual behaviour. In addition, users should not be informed about the real intention of the study. Informing users about phishing email study affects the data since it will increase users secure behaviour with emails (Wright et al., 2009). Therefore, we needed to send a phishing email to our participants without informing them about the real intention of our study. In addition, sending phishing emails to participants will allow us to classify participants as detectors or victims. The classification is done by recording participants' actions when they receive phishing emails.

Interviews generated in-depth, qualitative information about users' detection behaviour. Unlike surveys, which collect predetermined categories of information, interviews have the potential to reveal unexpected findings.

After the second survey, participants whom we had identified as detectors or victims were sent an email invitation to participate in a face-to-face interview. Those who agreed were contacted with a follow-up email to specify a suitable time. The interviews were conducted by the researcher in a designated meeting room and lasted between 20 and 30 minutes. Participants received a coffee voucher in appreciation for their time.

4.4 Data Analysis

This section describes the procedures used to analyse the quantitative and qualitative data, respectively

4.4.1 Quantitative data

Quantitative data about users' characteristics were analysed in the following steps: data preparation, data coding, production of codebook, computerised data entry, and error checking.

Three types of codes were used: codes for numerical data, codes for categorical data and codes for missing data (missing data was assigned to a specific numerical code). A codebook is a complete record of a series of codes. Each measurement is assigned to a code and this code is presented in a table. For example, one code used in the study is a 7 point Likert scale (Likert, 1932). Data are entered into a computer and prepared for the data analysis software. The data were entered into a spreadsheet in preparation for analysis by SPSS software. The group means approach was used to substitute some missing variables (De Vaus, 2002). Checking involved examining data for errors in the entry stage. Descriptive statistics were used to present the results of the analysis.

4.4.1.1 Descriptive statistics

Descriptive statistics enable the researcher to describe and compare variables from a numerical perspective (Saunders et al., 2009). They can provide measures such as standard deviation, mode, mean, median and variance in participants' responses and, importantly for our purposes, help to identify cause and effect relationships between dependent and independent variables through regression analysis. A t-test was used to find the difference between two means of the independent variables. Results were displayed in tables and figures, and the variables were firstly tested for reliability and validity.

4.4.1.2 Reliability and validity of results

Reliability refers to the extent to which an experiment or other procedure yields the same results if it is repeated (Saunders et al., 2009). Validity refers to the degree to which a study accurately measures what it is supposed to be measuring (Saunders et al., 2009). Several techniques of assessing reliability and validity were used in the present study. These included internal consistency, internal validity, content validity, criterion-related validity, construct validity and external validity. Relationships were measured using regression and structural equation modelling (SEM).

4.4.1.3 Correlation, regression and multiple regression analysis

The correlation coefficient is a measure of the strength of the relationship between two variables. It ranges between -1 (negative relationship), 0 (no relationship) and 1 (positive relationship). The correlation coefficient does not determine the direction of the causal relationship. The regression coefficient is a measure of the strength of the relationship between the dependent variable and one or more independent variables (Saunders et al., 2009). In the present study, there are two dependent variables (susceptibility and response) and several independent variables, so the use of multiple regression analysis is required.

4.4.1.4 Structural Equation Modelling (SEM)

SEM is a statistical technique that is used to test and validate the causal relationships between variables (Tembe, Hong, Murphy-Hill, Mayhorn, & Kelley, 2013). SEM can be used to confirm and explore proposed models which contain multiple dependent variables as well as the existence of latent variables (Ringle, Sarstedt, & Straub, 2012). SEM was used to test our research model and measure the relationships we developed.

4.4.2 Qualitative data

Qualitative data take the form of words rather than numbers. For analytical purposes, recorded interviews need to be accurately transcribed into written documents. We used the inductive approach, whereby the data were coded into categories that represented key themes and patterns or relationships (Braun & Clarke, 2006). We assessed reliability and validity through tests of credibility and confirmability.

The following sections describe in detail the instruments and procedures that were used in data collection.

4.5 Design of the Survey

Our hypothesis is that users' characteristics have a significant impact on their detection behaviour. The survey collected data on 12 characteristics:

1. Trust
2. Submissiveness
3. Perceived email experience and richness
4. Susceptibility
5. Big Five personality dimensions
6. Confirmation channels
7. Response
8. Age
9. Gender
10. Culture (language and nationality)
11. Usage (years in the Internet, hours in the Internet, years using the email service, years using the university email service and number of emails)
12. Internet activities (surfing, social and transactions)

4.5.1 Trust

High trust makes users give trust to entities which sometimes does not worth the given trust. Phishing emails are one of these entities which should not be trusted. In our research, we want to find the impact of this particular construct with users' behaviour with phishing emails. We measured participants' disposition to trust in general in both detectors and victims using instruments from McKnight et al. (2003) (see Table 9). Trust was measured on a 7 point Likert scale where 7 is strongly agree and 1 is strongly disagree.

Table 9: Trust items

Code	Item
Trust1	I usually trust people until they give me a reason not to trust them
Trust2	I generally give people the benefit of the doubt when I first meet them
Trust3	My typical approach is to trust new acquaintances until they prove I should not trust them

4.5.2 Submissiveness

Wright et al. (2009) suggested that the detectors in their experiment did not fall victim to the phishing email because they obeyed the instructions which had been given to them by the lecturer at the beginning of the semester and followed the rule of not disclosing their secret information to anyone. We measured submissiveness using instruments from Allan and Gilbert (1997) (see Table 10). Submissiveness was measured on a 5 point Likert scale where 5 is always and 1 is never.

Table 10: Submissiveness items

Code	Items
Missive1	I agree that I am wrong even though I know I'm not
Missive2	I do things because other people are doing them, rather than because I want to
Missive3	I would walk out of a shop without questioning, knowing that I had been short changed
Missive4	I let others criticise me or put me down without defending myself
Missive5	I do what is expected of me even when I don't want to
Missive6	If I try to speak and others continue, I shut up
Missive7	I continue to apologise for minor mistakes
Missive8	I listen quietly if people in authority say unpleasant things about me
Missive9	I am not able to tell my friends when I am angry with them
Missive10	At meetings and gatherings, I let others monopolise the conversation
Missive11	I don't like people to look straight at me when they are talking
Missive12	I say 'thank you' enthusiastically and repeatedly when someone does a small favour for me
Missive13	I avoid direct eye contact
Missive14	I avoid starting conversations at social gatherings
Missive15	I blush when people stare at me
Missive16	I pretend I am ill when declining an invitation

4.5.3 Perceived email experience and richness

Deception cues in a medium are more likely to be recognised by users with more experience in that medium (Carlson et al., 2004; Carlson & Zmud, 1999). Therefore, users with more experience in using the email system are more likely to identify phishing email cues. Perceived email experience and email richness were measured using instruments from Carlson and Zmud (1999) (see Table 11 and Table 12). Both characteristics were measured on a 7 point Likert scale where 7 is strongly agree and 1 is strongly disagree.

Table 11: Perceived email experience items

Code	Items
Email_Exp1	I am very experienced using e-mail
Email_Exp2	I feel that e-mail is easy to use
Email_Exp3	I feel competent using e-mail
Email_Exp4	I understand how to use all of the features of the e-mail system
Email_Exp5	I feel comfortable using e-mail
Email_Exp6	I feel that I am a novice using the e-mail system

Table 12: Perceived email richness items

Code	items
Email_rich1	E-mail allows my communication partner and me to give and receive timely feedback
Email_rich2	E-mail allows my communication partner and me to tailor our messages to our own personal requirements
Email_rich3	E-mail allows my communication partner and me to communicate a variety of different cues (such as emotional tone, attitude, or formality) in our messages
Email_rich4	E-mail allows my communication partner and me to use rich and varied language in our messages

4.5.4 Susceptibility

In the MDD, the first cognitive step in detection is activation, in which users suspect phishing emails. Users' subsequent behaviour will reflect their level of suspicion. To capture this important dimension, which we call susceptibility, we developed five phishing emails. Susceptibility was measured by the number of emails to which users chose to respond. A user who chooses to respond to all five will be categorised as highly susceptible.

The survey question asks users to pretend that they are a fictional person who has received these five emails. They are told that this person is a student with a bank account who also shops online and are asked to decide whether to respond to these emails or not. Most importantly, they have not been told that these are phishing emails, and the survey itself does not mention phishing emails to avoid priming participants.

The examples were carefully chosen to include both easily identified phishing emails (such as Nigerian 419 scams) and more complex ones such as personalised bank emails. All examples include features of phishing emails similar to those used in real phishing emails.

Participants were asked to play the role of a fictional person ('John' or 'Mohammed' for Australia and Saudi Arabia, respectively) who interacts with the companies represented in the phishing email examples. The companies themselves were well known in their respective countries. English was used in the emails for the Australian participants and Arabic for the Saudi Arabian participants.

The instruction for both studies was similar to each other and we show an example of the instruction used in the Australian study:

"Mr. John Douglas is a student at QUT University. He often shops from the Internet for which he uses his eBay and PayPal accounts. John verifies transactions done by bank using his online bank statement as he banks with CommBank. These organisations send emails about updates done on John's account and status. John always checks his email inbox and reads emails from QUT, eBay, PayPal and CommBank."

The five emails are described and displayed in the table below (see Table 13).

Table 13: Emails design

Emails	Personalised	Sender	Design	Response	Justification
Figure 13	No	Unknown	Text	Reply	Clear millions to charity
Figure 14	No	Known	Text	Reply	Maintenance
Figure 15	Yes	Known company	Text + Company logo	Click	Remove restriction
Figure 16	No	Known company	Text + Company logo	Click	Update users' information
Figure 17	No	Known bank	Text + Bank logo	Click	Verification

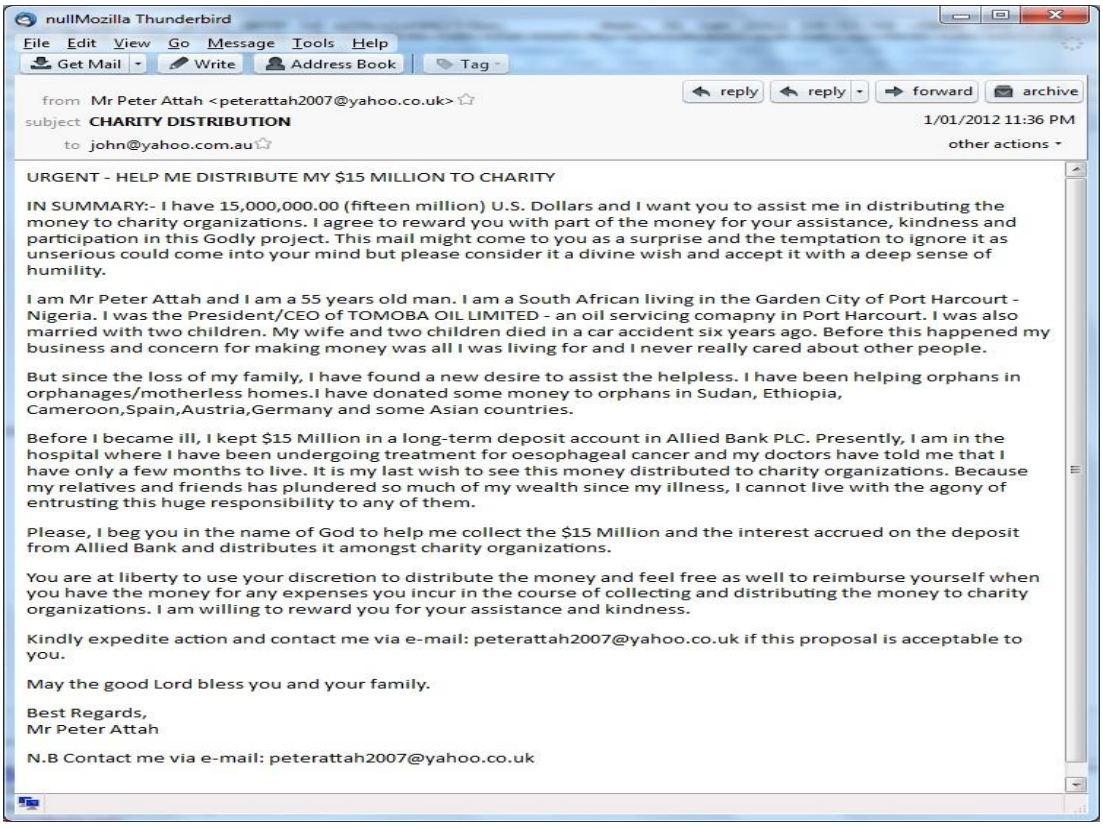

Figure 13: 419 scam email

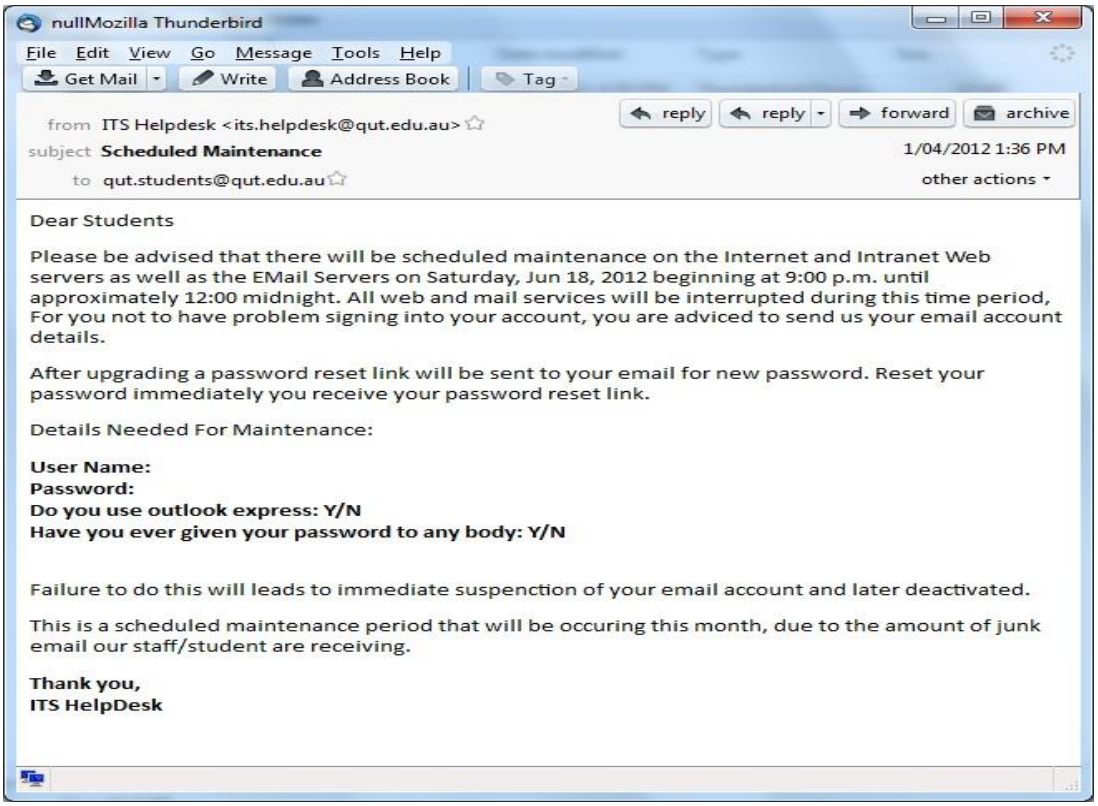

Figure 14: University email

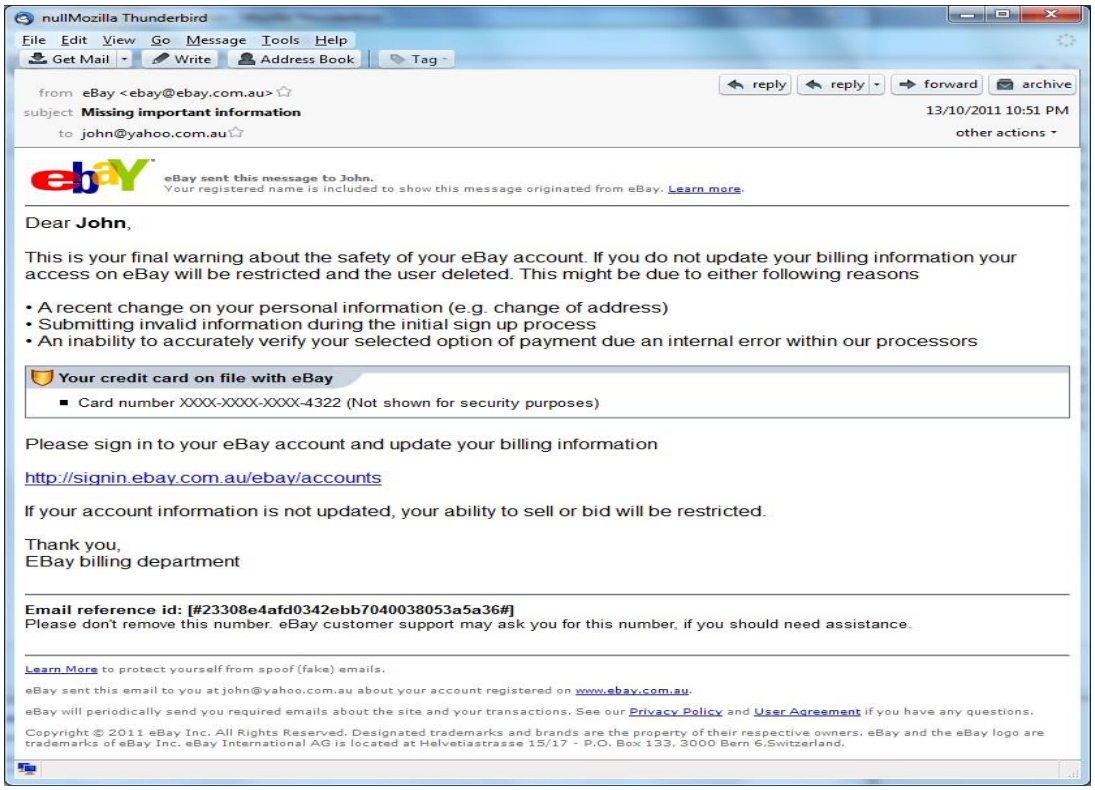

Figure 15: eBay email

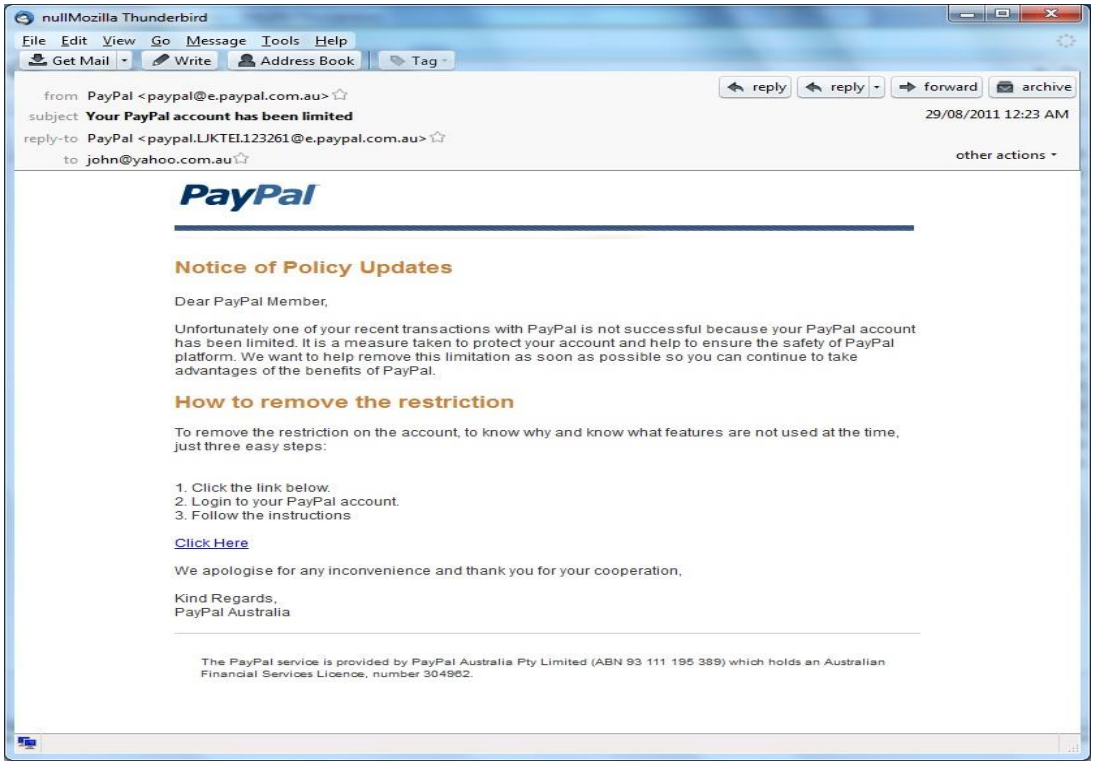

Figure 16: PayPal email

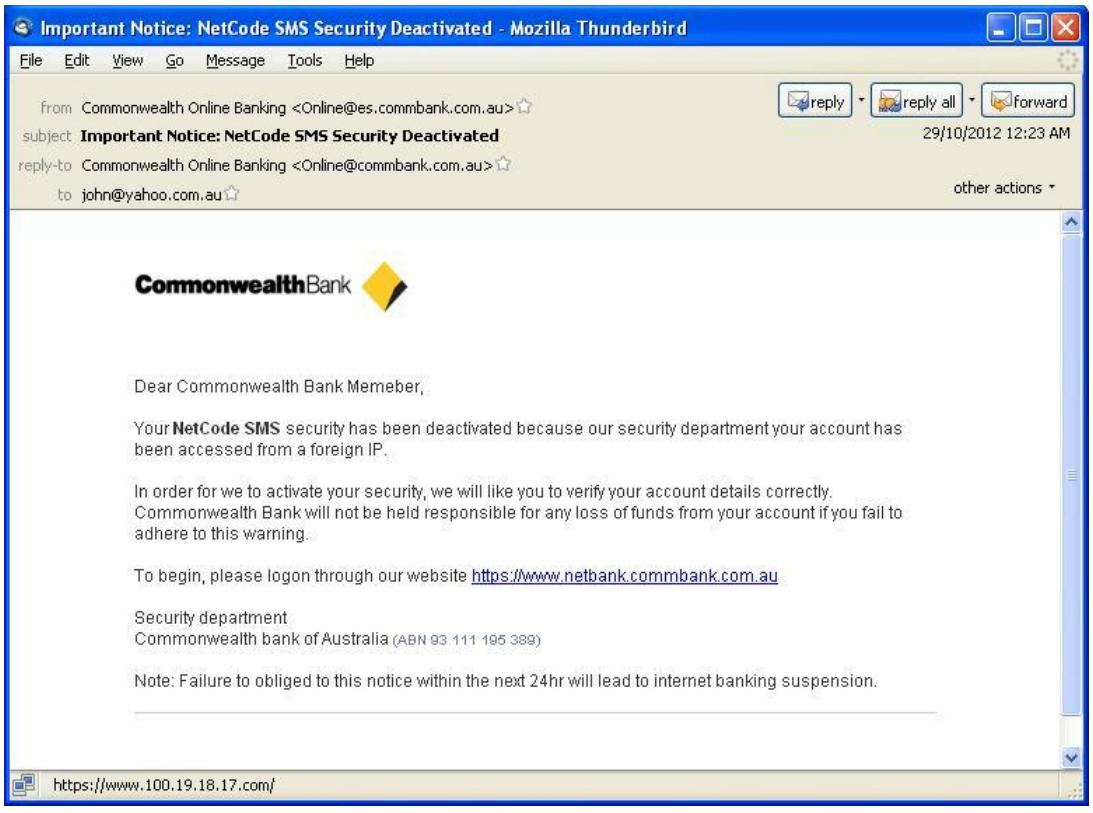

Figure 17: Bank email

4.5.5 Big Five personality dimensions

The Big Five personality dimensions are extraversion, agreeableness, conscientiousness, emotional stability and openness (Costa & McCrae, 1992). It has been suggested that variance in these dimensions may influence users' ability to detect phishing emails (Parrish Jr et al., 2009; Wright et al., 2009). Our research measured these personality dimensions in users using the TIPI measure (Gosling et al., 2003) (see Table 14), which uses a 7 point Likert scale (where 7 is strongly agree and 1 is strongly disagree). Each dimension is measured by the combination of two items and divided by two to form one dimension (GoslingLab, 2012). Please refer to the Appendix A question number 5 for more details.

Table 14: Big Five personality dimension items

Code	item
Extraversion 1	Extraverted, enthusiastic
Agreeableness 1	Critical, quarrelsome
Conscientiousness 1	Dependable, self-disciplined
Emotional stability 1	Anxious, easily upset
Openness 1	Open to new experiences, complex
Extraversion 2	Reserved, quiet
Agreeableness 2	Sympathetic, warm
Conscientiousness 2	Disorganized, careless
Emotional stability 2	Calm, emotionally stable
Openness 2	Conventional, uncreative

4.5.6 Confirmation channels

Users can be divided into three groups: 1) those who are able to detect a phishing email (detectors) and who mostly choose not to perform the requested action; 2) those who do not identify the email as a phishing email (victims) and who do not hesitate to perform the requested action; and 3) those who have doubts about the email and use various strategies to confirm or refute their suspicions.

Doubtful users use different ways of deciding about the authenticity of the suspected email. Our research focuses on their choice of confirmation channel. According to media richness theory and channel expansion theory, users are more

likely to detect deception in a rich medium. Therefore, we classified confirmation channels by their richness and asked users to report which channel they used to conduct their confirmation behaviour (see Table 15).

Table 15: Confirmation channel items

Code	Item
Channel1	Asking other persons face-to-face
Channel2	Asking other persons Telephone
Channel3	Asking other persons email
Channel4	Make a decision by yourself without consulting others
Channel5	Others

4.5.7 Response

This construct is measured by the actual response of users to the phishing email that was used in our research and which asked participants to reveal their passwords.

4.5.8 Age and Gender

Age and gender have been shown to influence users' ability to detect phishing emails (Jagatic et al., 2007; Kumaraguru et al., 2009; Sheng et al., 2010). Participants were divided into three age groups (see Table 16).

Table 16: Age and gender items

Code	Item
Age 1	18 -25
Age 2	26 -35
Age 3	Above 36
M	Male
F	Female

4.5.9 Culture

Culture has been found to play an important role in people's ability to detect lies from different cultures (Bond & Atoum, 2000; Bond et al., 1990). While culture has been under-researched in relation to phishing emails, it appears such detection is

easier in rich channels such as face-to-face interaction than in poor channels such as email. Therefore, it was suggested that culture have an impact of users' detection ability with phishing emails by our research.

Our research was conducted in two different countries: Saudi Arabia and Australia. Saudi Arabia was selected because it supports the research financially. Australia was selected because the research was conducted in Australia. In addition, both of these two countries have different culture. According to Hofstede (1993) these two countries are differ in their culture. Hofstede (1993) differentiate between cultures based on four dimensions: (1) power distance index (PDI), Individualism (IDV), uncertainty avoidance index (UAI), and masculinity versus femininity (MAS). The results for these dimensions are: 95 and 36 for (PDI), 25 and 90 for (IDV), 80 and 51 for (UAI), and 60 and 61 for (MAS) for both Saudi Arabian and Australian cultures respectively (Hofstede, 2001; Hofstede, 2011) . Observing the results above from Hofstede, it can be said that the Saudi Arabian culture is different from Australian culture. This difference between these two countries will allow our research to observe any differences caused by culture.

In Australian study, we identify culture through two items: first language and nationality (see Table 17). Language is important because it affects people's ability to spot deception cues such as typos or grammatical mistakes (Jakobsson et al., 2007). Nationality was selected because it has been shown that the national culture impacts on users' behaviour; some nationalities, for instance, demonstrate higher levels of loyalty to their companies than others (Hofstede, 1993). Such loyalty may influence users' susceptibility to certain types of phishing emails.

It was not considered necessary to measure these items in the Saudi Arabian study, since all participants had Arabic as their first language and Saudi Arabian as their nationality. Findings from the Saudi Arabian study were, however, compared with those from the Australian study to investigate the impact of culture.

Table 17: Culture items in Australia

Code	Item
English	English
Other	Other

Australian	Australian
Other	Other

4.5.10 Internet and email usage

The most important trigger for the detection of phishing emails is inconsistency between what users observe and what they expect (Buller & Burgoon, 1996). Phishing emails include information (cues) that aid detection of phishing emails. Expectations are generated by experience, which provides users with a baseline of knowledge for such comparison (Buller & Burgoon, 1996). Experience can be obtained from Internet usage and email usage.

Email usage is a subsection under Internet usage. Users who use email service are definitely using the Internet. However, not all users who surf the Internet is necessary has an email account. Furthermore, using the internet is not similar to using email. Internet usage is a type of communication between users and servers where emails can include other users. The type of information is also different for example website includes https or certificate for security measures. Email in other hand includes information such as email time and date, email address, email subject line, and sender name and contact details which can be used to validate emails. Therefore, we want to measure the experience developed by both Internet and email usage with users' ability to detect phishing emails.

Internet usage was measured by the number of years of Internet use and the number of hours of daily Internet use. Email usage was measured by the number of years participants had used the email service, the number of years they had used the university email service, and the number of emails they received per day. We measured years of university email service usage to investigate the relationship between detection ability and familiarity with a particular organisation (see Table 18).

Table 18: Internet and email usage items

Code	item
Y_Internet	How many years have you been using the Internet?
H_Internet	How many hours you usually spend in the Internet per day?

Y_Email	How many years you have been using the email service?
Y_Uni	How many years you have been using university email account?
No_Emails	What is the average number of emails you normally receive per day in your inboxes?

4.5.11 Internet activities

Some studies suggest that users' experience with the Internet significantly influences their ability to detect phishing emails (Downs et al., 2006; Kumaraguru et al., 2007) but others contradict these findings. Wright et al. (2009), for instance, reported no significant impact of online shopping on users' ability to detect deception. People use the Internet in different ways, and the experience of different activities may affect detection ability. For example, users may use Internet for reading newspapers. Such users may not develop a sense of security while using the Internet. In contrast, some users may use the Internet for banking and shopping. Such users may develop a sense of security which will affect their behaviour. In our research, we want to know whether such behaviour may affect users' ability to detect phishing emails.

In our research, Internet activities were measured differently in each study. In the first study (Saudi Arabia), participants were asked whether they perform one of the Internet activities or not (Checked/Unchecked). In the second study (Australia), the time spent on each Internet activities was measured using a 7 point Likert scale where 7 is more than 8 hours and 1 is none (Table 19).

The Saudi Arabian study was conducted first. Our interest was in whether performing online shopping affects users' vulnerability but we did not investigate the time spent in making such activity. A low level of usage may indicate relatively little experience with security issues, and vice versa. The Saudi Arabian results showed no significant differences between type of activity and users' vulnerability to phishing emails. Accordingly, in the Australian study, we included a measure of the time spent on each activity.

Table 19: Internet activities items

Code	Item
Activity 1	Surfing the Internet for knowledge (read only)
Activity 2	Making social activities (communicating with others)
Activity 3	Making online transactions (shopping – banking)

4.6 Phishing Email Experiment

This section describes the design and technical features of the phishing emails that were used in the experimental study to trick participants into revealing their passwords. Two types of phishing emails were tested: reply emails, which directly ask participants for their passwords, and click emails, which ask participants to click on a link in order to solve a problem in the blog server. They were designed to imitate real phishing emails. The main design features are:

1. Spoofing the "From" address line so that it is similar to a real university email.
2. Subject line is "Your (blog, email) privacy has been compromised" to capture users' attention and provoke fears about security.
3. Reply Nickname is similar to sender nickname.
4. Email reply prefix is similar to "From" prefix.
5. "Reply address" is hosted in a domain outside the university (malicious server).
6. The link in click email is hidden under the text "Click here".
7. The link points outside the university domain (malicious server).
8. The message has not been personalised for each student.
9. Message content presents students with a scenario involving event A which requires them to perform event B. In other words, there is a problem requiring ameliorative action.
10. The sender is addressed as "IT person, Subject team" without any communication details, as would be the case in a phishing email. It is not university practice to omit communication information.

Figure 18 and Figure 19 show images of the phishing emails used in the study conducted in Australia. Figure 20 and Figure 21 show images of the phishing emails used in the study conducted in Saudi Arabia.

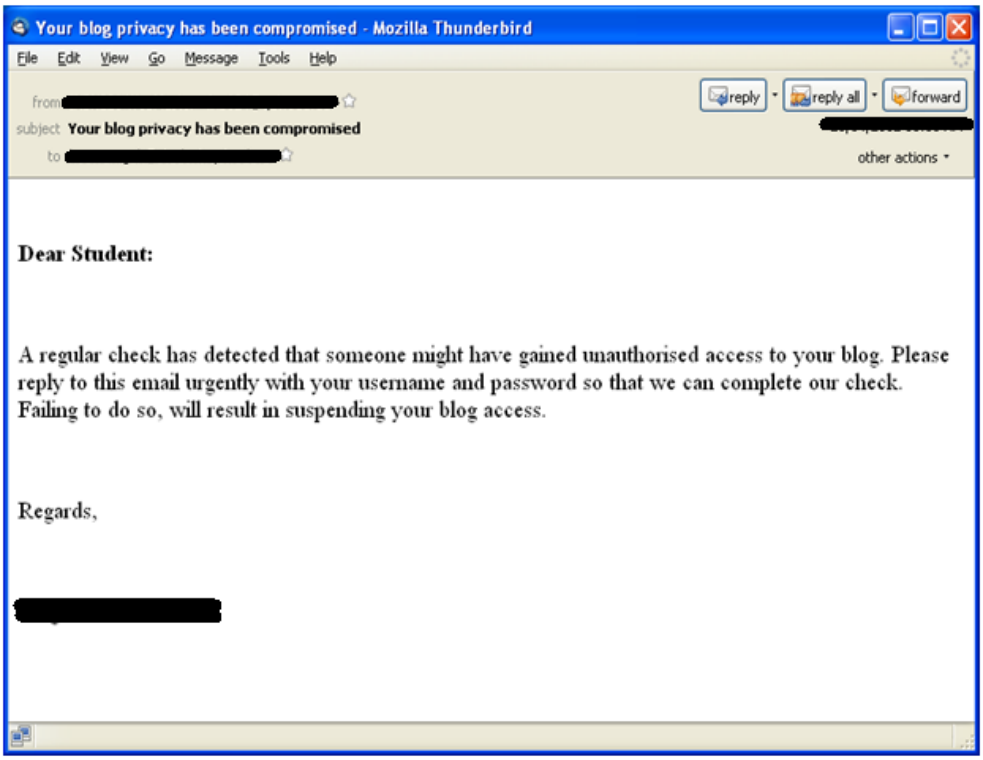

Figure 18: Reply phishing email (Australia)

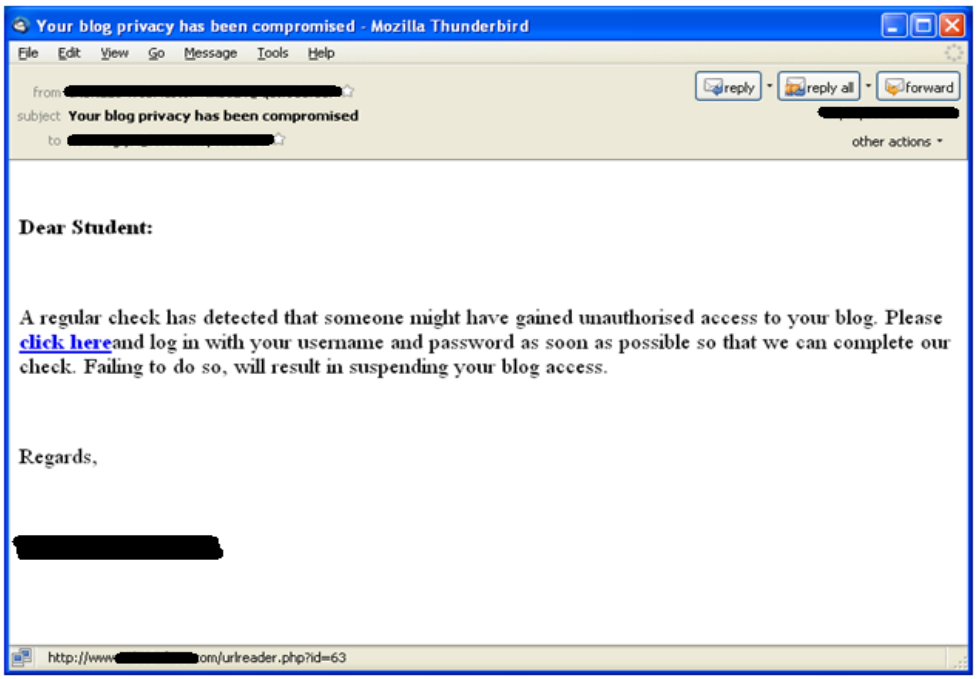

Figure 19: Click phishing email (Australia)

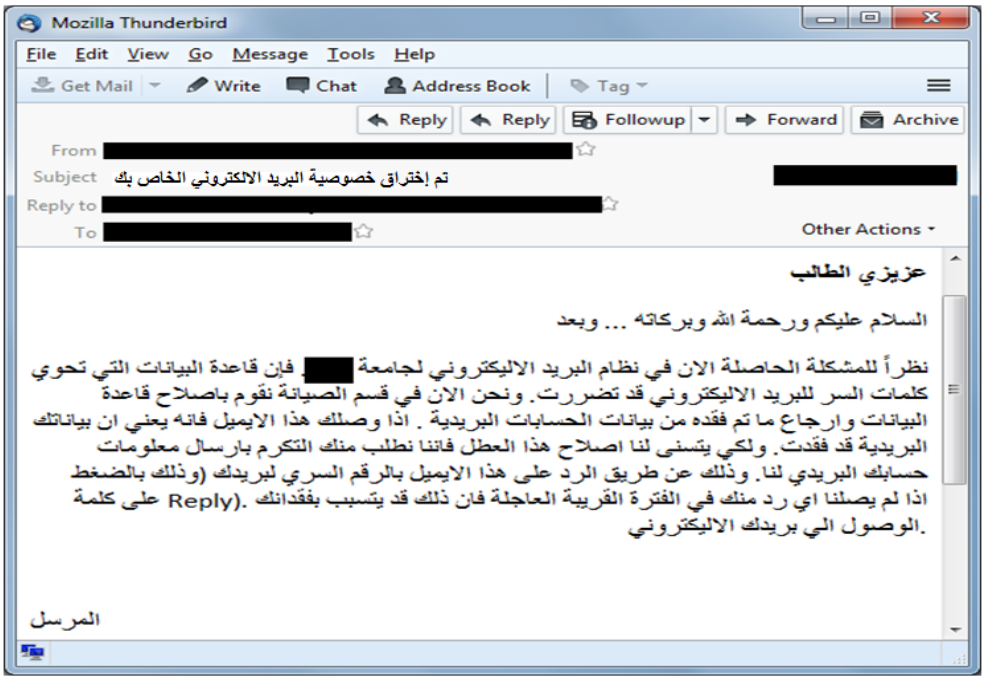

Figure 20: Reply email (Saudi Arabia)

Figure 21: Click email (Saudi Arabia)

4.6.1 Comparison with real phishing email design

This section compares the design features of our phishing emails with reported features of real phishing emails, as described by Wang et al. (2009) and Sharma (2010).

*Email argument quality***:** To ensure strong argument quality, the email begins by explaining why students have received it. The email reports a problem related to the receiver. This is the main structure of the argument. The problem has been discovered through the routine checking procedure used by the team who is supposed to maintain the accuracy and security of the blog or email. The problem is serious and needs to be resolved urgently. As similar to most phishing emails, the solution is already included in the email. Users are required to comply with the embedded request and will face a penalty if they do not.

Email title: This was designed to capture users' attention by highlighting the impact of the problem on users. We did not include the name of the organisation in the title because it can easily be included elsewhere. For example, the company name can be included in the metadata (e.g. address domain). We did not include 'Urgent' in the title because words like "urgent" are a sign of phishing emails and doing so may have reduced the likelihood that users would open the email.

Message appearance: The email did not include message appearance signs as reported by Wang et al. (2009). This is because messages sent to students from university employees do not display the company logo, third party icon or personalisation (except for communication details). Communication details were therefore excluded.

Assurance mechanisms: The email did not contain assurance mechanism signs (e.g. padlock icon or anti-fraud statement) since most emails from the university do not include these signs.

Source credibility: The most frequently reported source credibility features are: legitimate sender (prefix), legitimate sender domain and clear specific sender. The emails used in the Australian and Saudi Arabian experiments displayed a webmaster and IT personnel as the legitimate sender (prefix), respectively. The email domain

was identical to the domains of both universities. A specific sender was included at the end of the email. As explained above, the body of the email did not include telephone or email contact details or company logo.

Message credibility: The design incorporated all three of the most common forms of appeal: rational, emotional and motivational. In rational appeals, the email explains the reason why users should perform a certain action. Emotional appeals rely on fear; for example, informing users about unauthorised access to their accounts increases their fears about privacy and data integrity. Safety is the most commonly reported feature in motivational appeals. A report of unauthorised access to users' accounts motivates users to perform the action embedded in the email to maintain the safety of their account.

Message structure: The email included an explicit message, since this is more persuasive. Repetition and message order were not incorporated into the design because they would have limited impact in a short email. The phishing email used in the present study contained only the minimum amount of information considered necessary, namely: the reason for receiving the email, the requested action and the penalty for ignoring the email. Most of this information can be conveyed in one sentence. Providing more information may have negatively impacted on email persuasiveness.

Technical features: The information contained in the metadata was spoofed so as not to display any signs of phishing emails. Information included in the email header, however, can show that the email has not been sent from a university domain, as claimed, and does not have the same email address in the "reply to" bar with the email address in the "From" bar. The following is the email header in the phishing email.

Phishing email header (altered)

```
Delivered-To: XXX@ XXX.XXX.edu.sa or XXX@ XXX.XXX.edu.au
Received: by 11.67.159.65 with SMTP id x1cs333633pbq;
        Wed, 14 Dec 2012 20:13:47 -0800 (PST)
Received: by 11.17.126.181 with SMTP id
a11mr624877vvi.44.1121122216699;
        Wed, 14 Dec 2012 20:06:56 -0800 (PST)
Return-Path: <webmaster@servername.com>
Received: from servername (servername.com [89.27.111.222])
```

```
        by mx.XXX.com with ESMTPS id
n11si3333153vvh.58.2012.12.14.20.06.55
        (version=TLSv1/SSLv3 cipher=OTHER);
        Wed, 14 Dec 2012 20:06:56 -0800 (PST)
Received-SPF: pass (XXX.com: best guess record for domain of
webmaster@servername.com designates 89.27.111.222 as permitted
sender) client-ip=89.27.111.222;
Authentication-Results: mx.XXX.com; spf=pass (XXX.com: best guess
record for domain of webmaster@servername.com designates
89.27.111.222 as permitted sender) smtp.mail=
webmaster@servername.com
Received: from webmaster by servername.com with local (Exim 4.77)
        (envelope-from <webmaster@servername.com>)
        id 1Rc2ch-0004Fb-0k; Thu, 14 Dec 2012 20:06:56 -0800
To: XXX@ XXX.XXX.edu.sa or XXX@ XXX.XXX.edu.au
Subject: Your (blog, email) privacy has been compromised
From: Name <XXX@XXX.edu.sa or XXX@XXX.edu.au >
Reply-To: Name <webmaster@yahoo.com>
Content-Type: text/html
```

The original email header contained IP addresses that can identify the real sender and location of the email. IP addresses can be easily checked from several websites that provide this service free of charge. Other indications of illegitimacy are the sender domain (servername.com), which is not a university domain (authentic domain), and the reply email address (webmaster@yahoo.com).

4.7 Ethical Considerations

The conduct of this experiment required the use of deception (Jakobsson & Ratkiewicz, 2006) because it imitated real phishing email design. In other words, we sent phishing emails to participants. Clearly, this involves important ethical issues around the need to avoid harm to participants. Some phishing email studies have reported that some participants were upset by the deception (Kumaraguru et al., 2009; Kumaraguru et al., 2008). We needed to ensure that our experiment minimised the risk of harm by carefully controlling the outcome of participants' responses. Therefore, no important information was saved and the information was identified by number to maintain participants' anonymity.

We addressed these ethical concerns in several ways, taking into account the recommendations of Finn and Jakobsson (2007) regarding the design of phishing experiments. We did not request users to reveal secret information related to important accounts (e.g. enrolment, addresses) and we did not store their secret

information. The attacks developed during the project remain undisclosed and will be destroyed at the end of the research.

4.8 Pilot Study

Two pilot studies were conducted to identify the impact of priming on users' detection behaviour and to test the clarity and quality of the 1st and 2nd survey instruments.

It has been suggested that priming (warning users about the potential for deception) is a key factor that can trigger users to begin the process of detecting deception (Grazioli, 2004). For example, banks send emails to their clients informing them that the bank will never ask about passwords. This implies that any email claiming to come from the bank and asking about passwords is not legitimate. Such warnings can also come directly from managers to their employees. The main reason for priming is to increase users' awareness.

Since we were interested in investigating users' normal behaviour with phishing emails, we tested the impact of priming in two pilot studies with two different sets of participants. Participants were shown five phishing emails and asked two different questions. The first pilot study included 8 participants who were asked about the likelihood that they would respond to these emails using a 7 point Likert scale (where 1 is definitely ignore the email and 7 is definitely respond). The second pilot study involved 12 participants who were asked to rate the legitimacy of the emails on a 7 point Likert scale (where 1 is not a phishing email and 7 is a phishing email). Each group of participants was asked to justify their responses.

The results supported the idea that priming has an impact on users' ability to detect phishing emails. This suggested that we should avoid priming in the experiment, because some users may have no suspicions about the authenticity of phishing emails.

In addition to priming, which has been shown to impact on normal behaviour, we had to reduce the possible impact of interference by an authority. It was expected that some participants may ask the owner of the server (i.e. the lecturer) about the

phishing email. Any input from the lecturer could influence normal behaviour. If the lecturer advised some participants not to respond, this direct instruction may be delivered to other participants who had not yet seen the phishing email. Therefore, we delayed the lecturer response to any direct question about the phishing email by one week, until participants had sufficient time to see the phishing email and decide on an action.

4.8.1 Pilot study without priming (response to emails)

This pilot study suggested that participants who had not been informed that these were phishing emails did not base their decision (to respond or not) on a judgment of the email's legitimacy but on their interest in the content. Not one participant reported that s/he would not respond because these were phishing emails. Rather, some said they would not respond to some emails because they were irrelevant to them.

4.8.2 Pilot study with priming (response to phishing emails)

Participants who had been told to judge whether these were phishing emails behaved differently. They engaged in a decision-making process and looked for clues to judge the authenticity (or otherwise) of the emails. These findings suggest that some participants who suspected phishing emails may not have done so if they had not been told to judge their legitimacy. In real life, they may not detect phishing emails because detection needs to be triggered by suspicion. This is further supported by the findings of the first pilot study, in which no participants appear to have suspected that these were phishing emails. As a result, we avoided any form of priming in our study design in order to capture participants' normal behaviour.

The 20 participants in these pilot studies also provided comments that helped us to improve the survey instrument. After these changes were incorporated, data collection commenced, beginning with the Saudi Arabian study.

4.9 Differences between Saudi Arabian and Australian Studies

In broad terms, the research design was the same for the studies in Saudi Arabia and Australia (see Figure 22 and Figure 23). In both, the first stage involved a survey to collect data on users' characteristics and susceptibility to phishing emails. Next, phishing emails were sent to classify users into detectors and victims (the experiment). A second survey then collected data on confirmation channels. The last stage in both studies comprised interviews to collect more in-depth information about users' detection behaviour.

There were two minor differences between these studies: translation and type of information requested. The Saudi Arabian survey instruments were translated into Arabic (the national language of Saudi Arabia and first language of the Saudi Arabian participants). The information requested in Saudi Arabia was the participant's email password whereas in Australia it was the password for a private blog site that we set up (see Section 4.9.3). The blog was developed in Australian study to avoid any ethical issues related to expose participants' personal information. However, in Saudi Arabian study, blogs are not well used between students. Therefore, we asked about university email password. Both email and blog passwords are forms of credential information. These differences are discussed in more detail below.

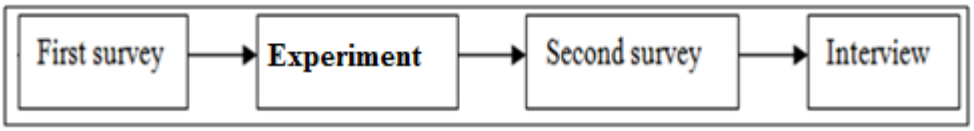

Figure 22: Saudi Arabian study methods

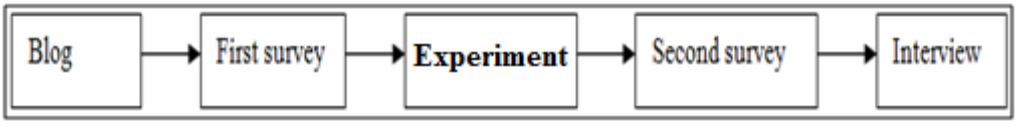

Figure 23. Australian study methods

4.9.1 Translation of Saudi Arabian survey

The survey and related instruments were initially developed in English. Most Saudi students have very limited knowledge of English. The translation process proceeded as follows benefiting from Brislin method (Brislin, 1983):

1. The survey was developed in English then translated from English to Arabic by a specialised translation service.
2. The resulting Arabic survey was again translated from Arabic to English by a different translation service to perform comparison.
3. The two English versions were compared to identify any differences, especially in relation to changes in meaning. Where discrepancies were found, the Arabic version was amended to ensure it captured the original meaning.
4. The final Arabic survey was sent to an Arabic editor for the final correction of any mistakes in spelling or grammar.

4.9.2 Activation of university email service for Saudi Arabian students

Some Saudi Arabian participants were asked to activate their university email because they had not already done so. This request was made by a lecturer who contributed to our research project. The activation was requested in such a way to avoid priming participants about phishing emails; the lecturer advised students that they needed to activate their university email to receive their marks and some unit instructions. This encouraged students who had not activated their university email to do so. In the month following activation, students received emails from the lecturer that included some course materials and exam marks.

During this month students also received emails from the university, which allowed them to become familiar with the university email. During this month, students who had not activated their email the system returned undelivered emails to the lecturer. Undelivered email notice allowed the research team to exclude such students from the study sample. During the second month from activation, the research phishing email was sent to students.

To ensure that all participants had enough time to see the phishing email, the lecturer told students that he would be sending the marks from the second

examination during the following week (i.e. when the phishing email would be sent). Thus participants would be encouraged to check their inboxes during that week. This was necessary because some students may not otherwise have opened their emails at that time.

It was important to minimise the gap between sending and receiving the phishing email because it emphasised the importance of performing the requested action as soon as possible. If there was a long delay (of a week or more), students may be less motivated to perform the action. At no time did the lecturer mention the phishing email in his classes, since doing so may have led some students to interpret the reference as validating the authenticity of the email.

4.9.3 Development of blog for Australian participants

The Australian experiment had to adopt a different approach to the provision of credential information. In Australia (unlike in Saudi Arabia), students' email credentials are linked to sensitive university information (e.g. addresses, phone numbers). However, the phishing email used in our experiment is sent to students email similar to the experiment in Saudi Arabia.

The type of expected attackers in terms of the blog can be limited to the number of people who knows about the blog (i.e. students). While in email, the expected attackers can be wider than the number of expected attackers in the blog. Especially, the blog was designed to be accessed inside the university network. In our research, the phishing email is designed to target specific users in an organisation. Therefore, the attacker is more expected to know some information about the targeted victims. In addition, participants who lose their passwords are deceived by the phishing email which makes them believe its legitimacy. Since, we have emphasised the importance of keeping the password secret. Furthermore, the percentage of victims fall in our experiment is in the range of expected victims fall victims in phishing emails studies which are not limited to blog (Sheng et al., 2007; Zhang, Luo, Burd, & Seazzu, 2012).

In both Saudi Arabian and Australian study, the design of the phishing email is similar to each other (see Section 4.6). The only difference between these two studies is the type of the requested password in the phishing email. In Saudi Arabia the

password is used for emails while in Australia the password is used for the blog. It can be said that the importance of the email password is not similar to blog password. However, we applied the following procedures to increase the importance of the blog password. These procedures emphasise the weight of blog privacy.

In order to ensure privacy, we created a blog on the Internet with the assistance of the university's IT unit. The blog could not be accessed outside the university network. Students were required to submit an article to the blog for assessment. These articles were private. Students could not view other students' posts. To gain credit for the unit, students had to write several articles in their own account in the blog. No priming was involved, since students had not been told that the blog was being used to conduct a phishing email experiment.

To access their account in the blog, students were given usernames and passwords. They were informed not to give their credentials to anyone and that the blog was private (i.e. students could not see each other's articles). These measures were taken to ensure that students who revealed their credentials were really victims of the phishing email and not simply careless about their credentials.

The privacy of the blog was important for students to make them think about protecting their posts. The lecturer emphasised that plagiarism would be taken seriously and any student caught plagiarising would be dealt with under the university's plagiarism policy, in which sanctions include suspension for the current semester. Both the student who plagiarised and the student whose work was plagiarised would be affected, since the latter had allowed access to her/his account. The default status for a new post was set to be private, meaning that other students cannot see any new posts. To avoid sanctions, therefore, students must ensure that their account is protected.

The process of making the blog private is explained below. By default, WordPress does not support this, so we went to the file codes and edited them to ensure all posts from students were private. The following are the steps we followed to ensure that all posts were private. This was done so that we were able to establish that any case of plagiarism was the result of account theft or of students' carelessness. It also highlighted the importance of protecting account information.

First, the file “meta-boxes.php” was edited. In this file, the default setting for the post is set to public. This was changed to private. This ensures that any new post to the blog will be private. Students cannot change the status to public.

We also disabled the edit time and date function so that post date and time cannot be changed. This step would allow us to detect any student who might attempt to copy others’ articles.

The function that allows students to quick edit their post was also disabled. This function allows students to change the status to public, which contravenes the blog rules.

The file “functions.php” in the active theme was edited. Themes have a widget which is installed as default in the dashboard and appears when users login to their account. This function allows users to post their articles directly to the blog. It has only one status—public—that has to be disabled to enforce private posts. Deleting the widget from the theme prevents students from posting articles publicly.

By editing these files in the server, we ensured that no student could legally access other students’ posts. Enforcing this rule satisfies the unit requirement that “assignments should be protected from other students”. At the same time, it served the research purpose of emphasising the importance of protecting students’ private information on the blog.

4.9.4 Content of phishing emails

The phishing email was sent on behalf of an authentic IT person who administered the university network and blog maintenance team in the Saudi Arabian and Australian experiments, respectively. This had two main goals. The first was to highlight the fact that the email came from the university (since the identified problem occurred in the email or blog system). Phishing emails purport to come from an organisation known to receivers. For example, phishing email attacks targeting a particular bank close their message with the name of a known employee in the bank or its security department. The second goal was to identify detectors who use this kind of information, since failure to provide specific information about the sender should arouse users’ suspicion.

The phishing email informed participants about a problem in the blog that had damaged some system information in which students' account information (i.e. passwords) was held. It emphasised that the recipient of the email had been affected by this problem and needed to act quickly to resolve it. Following this explanation, participants were presented with the solution, as in a real phishing email. Because the research aimed to identify the impact of the type of the phishing email on participants' responses, two different kinds of email were sent, each presenting a possible action: replying to the email address with the requested information or clicking on a link embedded in the phishing email.

The design of the phishing email imitated that of real phishing emails. The "From" address was spoofed so that it appeared similar to the university's domain name (a trusted address). The message reported a current problem in the system which had damaged the student database (including passwords). Students were asked to resolve the problem by responding with their passwords. As noted above, two different kinds of email were sent, each presenting a possible action of response: replying to the email address with the requested information or clicking on a link embedded in the phishing email. Failure to respond, the message claimed, would result in suspension of the student's account.

4.9.5 Identification of victims

In reply phishing emails, when participants chose to reply to the phishing email they believed they were replying to the email address of the sender (i.e. the university, which appears in the address bar). Clicking on reply generated a prompt that has the same sender name but a different email address. Only cautious participants would notice the difference between received address ("From") and sending address ("Reply to"). This design feature allowed us to capture participants who check email addresses before sending emails.

Emails from participants who choose to reply are sent to the address specified in the phishing email, which is controlled by the research team. In this way, we can identify victims and match their responses to the phishing email with their responses to the survey.

In the click phishing email, participants are requested to click on an embedded link. The email appears to come from an authentic entity in the university but the link points to a different address, outside the university, which can be identified by moving the mouse over the link. The link is hidden as a hyperlink behind the "Click here" text. A hyperlink is used to avoid email filters, which compare URL addresses with displayed addresses, and to prevent participants from making their own comparison.

Each participant was assigned a unique ID number. When participants click on the embedded link in the phishing email, they will be connected to a website created for this research. This website captures participants' ID number and sends it to an email address managed by the researcher. The website then redirects the connection to a real university website where email or blog passwords can be reset. This is similar to the action of phishing emails, which ask users to connect to a malicious website, where their secret information is captured, and then connect them back to a legitimate website to reduce the chances of detection. Thus, users do not know that they have fallen victim to a phishing attack. If they did become aware of this, they may deactivate their accounts or change their secret information to make the lost information useless.

4.10 Summary

This chapter has presented the research design and described the quantitative and qualitative methods employed in the study. Differences in the design of the Australian and Saudi Arabian studies were explained and justified. The instruments and procedures used to collect data and identify detectors and victims were described in detail.

Chapter 5: Quantitative Analysis

A total of 780 participants, 350 from Saudi Arabia and 430 from Australia, were initially targeted in this study. Only those participants who successfully completed the two surveys and the experiment used in our research are included in the analysis. The final sample comprised 383 participants, 196 from Saudi Arabia and 187 from Australia.

This chapter describes the quantitative data analysis procedures employed in this study and presents the descriptive outcomes from the survey. It examines reliability and validity of the survey instruments and explains how SEM was used to measure the overall research model.

We used SPSS software version 21 and SmartPLS software version 21 to analyse the data from both surveys and the experiment. The final model was analysed with structural equation modelling (SEM) using R software with Lavaan packages. The results of this analysis are presented in detail.

5.1 Data Preparation

Data preparation is an important step to make data ready for analysis. The data were prepared for analysis following the four steps suggested by Fink (2009): data coding, data entry, data cleaning, and finding missing values. These steps are explained below:

1. Data coding: Produce a code book for the data. For example, the three age groups (18-25), (26-35) and (36 and above) were coded age1, 2 and 3 respectively.
2. The survey was conducted online, which means that the data were entered electronically. However, the dataset had to be cleaned of unrelated entries such as questions.

3. Data eligibility: This step involves an examination for ineligible data. It has two phases: data eligibility and response eligibility. For example, data eligibility for scales in some survey questions was from 1 to 7. We ensured that the answers to these question range between 1 and 7. Response eligibility involves making sure that answers are not exactly the same for all questions.
4. Missing values: In the case of participants who did not complete and submit all the required questions in the two surveys, the data were considered incomplete. Answers from these participants were omitted from the dataset.
5. Negative statements were reversed to avoid extremity bias.
6. Raw data were first entered into a Microsoft Excel file and then exported to SPSS statistical software.
7. An additional test was conducted using SPSS (version 21) which produced frequencies of the entered data so they could be examined for missing values and outlier responses.

5.2 Descriptive Outcomes

This section summarises the descriptive data, beginning with the demographic items for both studies.

5.2.1 Demographic items

There was no diversity in the demographic characteristics of the Saudi Arabian participants, all of whom belonged to the first age group, were male, spoke Arabic as their first language and gave Saudi Arabian as their nationality. This mainly reflects the fact that most Saudi Arabian universities only accept Saudi Arabian students. Usage and Internet activities showed some variance. On the other hand, there was variance in the demographic items in the Australian study, as explained below, since Australian universities are open to local and international students from different cultures.

5.2.1.1 Age, gender and culture

In the Australian study, two-thirds (69.5%) of the 187 participants were under 26 years of age and 77.5% (N=145) were male (Table 20). Some 57.2% (N=107) spoke English as their first language and 58.3% (N=109) identified their nationality as Australian (Table 21).

Table 20: Age and Gender

Age	Frequency	Percent	Gender	Frequency	Percent
18-25	130	69.5	Male	145	77.5
26-35	57	30.5	Female	42	22.5

Table 21: Culture (Language and Nationality)

Language	Frequency	Percent	Nationality	Frequency	Percent
English	107	57.2	Australian	109	58.3
Not English	80	42.8	Not Australian	78	41.7

5.2.1.2 Internet and email usage

Participants from both studies were asked five questions about their Internet and email usage (Table 22).

Table 22: Descriptive statistics for usage

	Saudi Arabia	Australia
Statistics	**Mean**	**Mean**
Number of years using the Internet	7.02	9.92
Number of hours per day spent on the Internet	3.19	5.37
Number of years using email service	5.80	8.64
Number of years using university email service	1.49	1.60
Average number of emails received per day	10.2	10.43

As shown in Table 22, Saudi Arabian participants had used the Internet on average for about 7 years, spent about 3.2 hours per day on the Internet, had used an email service for about 6 years, had used a university email service for 1.5 years, and received about 10 emails per day. Australian participants, on average, had used the Internet for about 10 years, spent around 5 hours per day on the Internet, had used an email service for about 9 years, had used a university email service for 1.6 years, and received about 10 emails per day.

5.2.1.3 Internet activities

These questions were designed to identify the relationship between users Internet activities and their detection behaviour in relation to phishing emails. Previous studies have suggested that experience with activities that involve secret information, such as online shopping, affects users' ability to detect phishing emails (Kumaraguru et al., 2007). The present study sought to identify the impact of certain activities on users' detection behaviour, but the measurement in the questions in the Saudi Arabian and Australian studies were slightly different (the reason for the differences is explained in Section 4.5.11).

In Saudi Arabia, participants were asked to indicate their response (Yes, No) to three items asking about their main use of the Internet. Australian participants were asked to rate themselves on three items that described Internet activities using a 7 point Likert time-based rating scale (None, 1-30min, 30-60min, 1-2hrs, 2-4hrs, 4-8hrs, More than 8hrs).

The results from this question were quite similar in both studies; that is, there was little difference in Internet activities between the two groups. Both Saudi Arabian and Australian participants were most likely to report that they mainly surfed the Internet for knowledge and least likely to report that they mainly used it for online transactions.

5.2.2 Trust

Participants from both studies were asked to rate three items related to trusting other people, using a 7 point Likert agreement scale (Strongly disagree, Moderately

disagree, Disagree a little, Neither agree nor disagree, Agree a little, Moderately agree, Strongly agree). The results are shown in Table 23.

Table 23: Descriptive statistics for the three trust items

	Saudi Arabia	Australia
Statistics	**Mean**	**Mean**
Usually trust people until have a reason not to trust them	4.89	4.90
My typical approach is to trust new individuals until they prove I should not trust them	4.57	4.78
Generally give people benefit of doubt when first meet them	4.09	4.72

As shown in Table 23, Saudi Arabian participants were most likely to agree that they usually trusted people until they had a reason not to do so. They were least likely to agree that they generally gave people the benefit of the doubt when first meeting them. Australian participants were most likely to agree that they usually trusted people until they had a reason not to do so. They were least likely to agree that they usually trust people until they have a reason not to trust them. In general, Saudi Arabian and Australian participants fall in the category neither agree nor disagree to trust people.

5.2.3 Submissiveness

Participants from both studies were asked to rate themselves in terms of 16 items that described various kinds of submissive behaviours. They did so using a 5 point Likert frequency rating scale (Never, Rarely, Sometimes, Mostly, and Always). The results are shown in Table 24.

Table 24: Descriptive statistics for 16 submissiveness items

	Saudi Arabia	Australia
Statistics	Mean	Mean
Say thank you enthusiastically & repeatedly when someone does a small favour	4.20	4.14
If I try to speak and others continue, I shut up	3.73	4.21
I continue to apologise for minor mistakes	3.28	4.06
I do what is expected of me even when I don't want to	3.18	4.44
At meetings & gatherings I let others monopolise conversation	3.06	3.84
I am not able to tell my friends when I am angry with them	2.97	3.88
I avoid starting conversations at social gatherings	2.92	3.63
I avoid direct eye contact	2.80	3.56
I would walk out of shop without question knowing I'd been short-changed	2.79	3.80
I agree I'm wrong even when know I'm not	2.71	3.63
I blush when people stare at me	2.64	3.52
I pretend I am ill when declining an invitation	2.58	3.60
I don't like people to look straight at me when they are talking	2.55	3.52
I listen quietly if people in authority say unpleasant things about me	2.48	3.97
I do things because others are doing them rather than because I want to	2.42	3.66
Let others criticise me or put me down without defending myself	2.26	3.52

As shown in Table 24, Saudi Arabian participants were most likely to state that they say thank you enthusiastically and repeatedly when someone does them a small favour. They were least likely to state that they let others criticise them or put them down without defending themselves. Australian participants were most likely to state that they do what is expected even when they do not want to. They were least likely to let others criticise them or put them down without defending themselves.

5.2.4 Perceived email experience

Participants from both studies were asked to rate six items listing various aspects of email experience, with responses utilising the 7 point level of agreement Likert rating scale initially used for Trust. The results are shown in Table 25.

Table 25: Descriptive statistics for six items related to email experience

	Saudi Arabia	Australia
Statistics	Mean	Mean
Feel that email is easy to use	5.70	5.48
Feel competent using email	5.62	5.18
Feel comfortable using email	5.13	5.71
Very experienced at using email	4.92	5.40
Understand how to use all the features of email system	4.81	5.36
Feel that am a novice at using email system	3.01	2.30

As shown in Table 25, Saudi Arabian participants were most likely to agree that email is easy to use and that they feel competent using email. They were least likely to agree that they felt they were novices at using the email system. Australian participants were most likely to agree that they feel comfortable using email. They were least likely to agree that they felt they were novices at using the email system.

5.2.5 Perceived email richness

Participants from both studies were asked to rate four items describing various aspects of the richness of the (shared) email experience with responses utilising the 7 point level of agreement Likert rating scale initially used for Trust. The results are shown in Table 26.

Table 26: Descriptive statistics for four items related to email richness

	Saudi Arabia	Australia
Statistics	Mean	Mean
Email allows communication partner & me to tailor messages to personal requirements	5.08	4.44
Email allows communication partner & me to give and receive timely feedback	4.97	4.55
Email allows communication partner & me to use rich and varied language in messages	4.97	3.97
Email allows communication partner & me to communicate a variety of cues	4.90	3.84

As shown in Table 26, Saudi Arabian participants were most likely to agree that email allows communication partner and me to tailor messages to personal requirements. They were least likely to agree that email allows communication partner and me to communicate a variety of cues. Australian participants were most likely to agree that email allows communication partner and me to receive timely feedback and to tailor messages to personal requirements. They were least likely to agree that email allows communication partner and me to communicate a variety of cues. Table 26 suggests that both groups of participants perceived emails as a rich channel.

5.2.6 Susceptibility

Participants from both studies were asked to rate five phishing emails from five different sources using a 7 point likelihood of response Likert scale (Definitely will delete or ignore the email, Most likely will ignore or delete the email, Maybe will ignore or delete the email, Do not know, Maybe will respond, Most likely would respond, Definitely would respond). The results are shown in Table 27.

Table 27: Descriptive statistics for five items related to susceptibility

	Saudi Arabia	**Australia**
Statistics	Mean	Mean
How likely that will click on bank link	4.79	4.84
How likely that will click on eBay link	4.08	4.34
How likely that will click on PayPal link	3.63	3.70
How likely that will reply to Uni. email	3.46	3.16
How likely that will reply to scam	3.40	3.34

As shown in Table 27, both groups of participants were most likely to respond to the email if it contained a bank link. They were least likely to respond to the email if it is a scam or university email.

5.2.7 Big Five personality dimensions

Participants from both studies were asked to rate themselves in terms of five personality traits, based here on 10 summary descriptive items (where answers to a

larger array of items are summarised in terms of the five personality traits). These items are based on the Big Five personality traits (see Section 4.5.5).

Participants rated themselves on the 10 summary items on a 7 point Likert scale (Strongly disagree, Moderately disagree, Disagree a little, Neither agree nor disagree, Agree a little, Moderately agree, Strongly agree). The results are shown in Table 28.

Table 28: Descriptive statistics for the 10 personality dimension items

	Saudi Arabia	**Australia**
Statistics	Mean	Mean
Dependable, self-disciplined	5.70	4.77
Sympathetic, warm	5.61	4.03
Extraverted, enthusiastic	5.41	4.49
Reserved, quiet	5.27	3.82
Calm, emotionally stable	4.96	4.63
Open to new experiences, complex	4.71	5.19
Anxious, easily upset	4.33	3.56
Critical, quarrelsome	3.51	4.10
Conventional, uncreative	3.36	2.72
Disorganised, careless	3.28	3.09

As shown in Table 28, Saudi Arabian participants were most likely to agree that they were dependable and self-disciplined, sympathetic and warm, or extraverted and enthusiastic. They were least likely to agree that they were disorganised and careless, conventional and uncreative, or critical and quarrelsome. Australian participants were most likely to agree that they were open to new experiences, complex, or dependable and self-disciplined. They were least likely to agree that they were conventional and uncreative, or disorganised and careless.

In this report of outcomes, the 10 items were combined in pairs to obtain scores related to each of the five personality dimensions. The procedure used was to add related pairs, with the negative item reverse scored, and to divide the resulting total by two to obtain the mean score (GoslingLab, 2012). The results are presented in Table 29.

Table 29: Descriptive statistics for Big Five personality dimension scores

	Saudi Arabia	Australia
Statistics	Mean	Mean
Conscientiousness mean score	5.186	4.54
Openness mean score	4.663	5.23
Extraversion mean score	4.069	4.33
Emotional mean score	3.688	3.29
Agreeableness mean score	2.964	3.97

As indicated in Table 29, Saudi Arabian participants were most likely to agree that they were conscientious, open and extraverted and least likely to agree that they were emotional or agreeable. Australian participants were most likely to agree that they were open and least likely to agree that they were agreeable and emotional.

5.2.8 Confirmation Channels

Participants from both studies were asked to indicate whether or not they took one of four ways to check the authenticity of the phishing email used in our experiment. The results are shown in Table 30.

Table 30: Descriptive statistics for four items related to confirming the authenticity of emails

	Saudi Arabia	Australia
Statistics	Mean	Mean
Confirm by asking others via telephone	0.70	0.15
Confirm by asking others face-to-face	0.23	0.22
Confirm by asking others by email	0.05	0.21
Confirm by making decision without consulting others	0.01	0.31

As indicated in Table 30, Saudi Arabian participants were most likely to confirm by asking others via the telephone. They were least likely to do so by

making decisions without consulting others. Australian participants were most likely to confirm by making decisions without consulting others. They were least likely to do so by asking others via telephone.

5.2.9 Response

This is the final action in users' detection behaviour. This action determines victims who have actually responded to the phishing emails used in our research. We sent two types of phishing emails to participants: reply emails and click emails. The score is calculated based on whether or not users responded to these phishing emails.

In the Saudi Arabian study, of the 350 targeted participants, 4% (N=14)[8] responded to the phishing email used in our research. This percentage fell in the normal range for the percentage of users who fall victim to phishing email incidents (Jakobsson & Ratkiewicz, 2006; Knight, 2004; Pettey, 2006).

In the Australian study, of the 430 targeted participants, 26% (N=112)[8] responded to the phishing email. This percentage is higher than the percentage of victims in the Saudi Arabian study as well as higher than the normal estimated percentage (Pettey, 2006). However, it is in the normal range for users who become victims in an experimental setting (Sheng et al., 2007; Zhang et al., 2012). Sheng et al. (2007) reported that nearly 38% of their participants fell victim in their experiment, while Zhange et al. (2012) reported that 36% did so. These differences are discussed in more details in Chapter 7 (see Section 7.2.1).

We recorded the first Saudi Arabian victim 24 hours after the phishing email had been sent, while the first response from an Australian victim came during the first five minutes. In fact, the majority of Australian victims responded in the first four hours.

5.3 Demographic Analysis

As explained in Section 5.2.1, the Saudi Arabian participants did not display variance in the three demographic variables of age, gender and culture. The low

[8] This number includes all victims in this study even those who did not complete all data collection.

variance resulted in these variables result in omitting them from further analysis. These participants, however, showed variance in the items on usage and Internet activities. The analysis showed that there is no significant impact of these variables on users being victims. This is mainly because the number of victims in the Saudi Arabian study was very low (4%). On the other hand, the Australian study showed a variance between the items included in each variable. This variance led us to analyse the demographic variables in the Australian study. The results are presented below.

5.3.1 Age

We used Sheng et al.'s (2010) categorisation of age groups (18-25, 26-35, 36 and above). As Table 31 shows, only two categories were represented in the Australian study (18-25, 26-35). The Chi-square test was used to test the relationship between age and users' response to the phishing email. It showed a significant relationship between young users and response to the phishing email (see Table 32). This supports previous findings that younger users are more likely to be more vulnerable to phishing emails than other age groups (Sheng et al., 2010). Figure 24 shows the frequency between users' age and response (action).

Table 31: Frequencies age

			Action		Total
			Victim	Detector	
Age	18-25	Count	58	72	130
		Expected Count	50.7	79.3	130.0
	26-35	Count	15	42	57
		Expected Count	22.3	34.7	57.0
Total		Count	73	114	187
		Expected Count	73.0	114.0	187.0

Table 32: Chi-square test age

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	5.576	1	.018		
Continuity Correction	4.833	1	.028		
Likelihood Ratio	5.765	1	.016		
Fisher's Exact Test				.022	.013
Linear-by-Linear Association	5.546	1	.019		
N of Valid Cases	187				

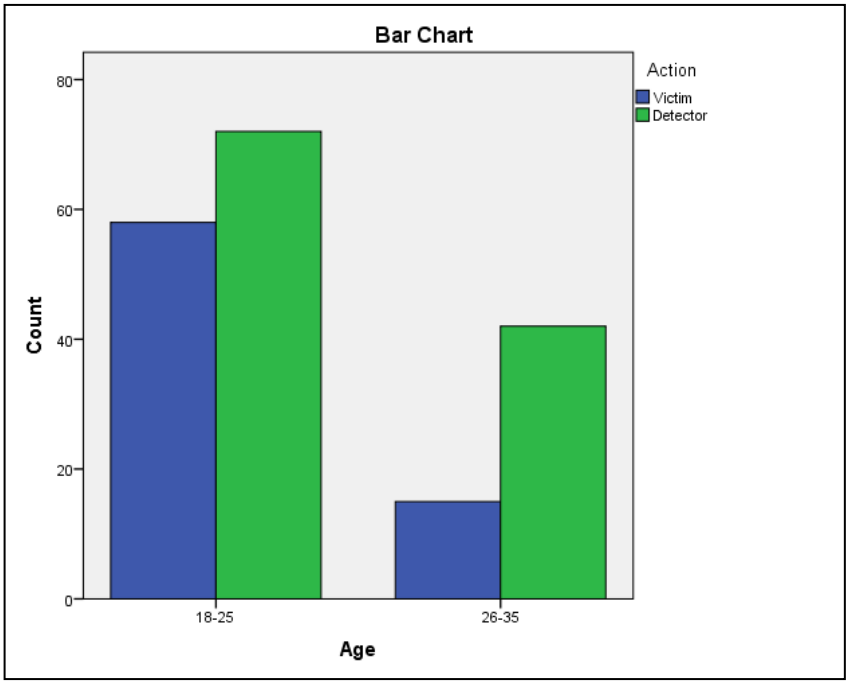

Figure 24: Frequencies chart age

5.3.2 Gender

The Australian study showed a difference in users' gender, with males representing 78% of the sample. The results in Table 33 show that males are less vulnerable to phishing emails than females. The Chi-square test shows that the difference due to gender is not significant (see Table 34). This finding is consistent with the results obtained by Sheng et al. (2010), who found gender was not a significant predictor of users being victims. Figure 25 shows the frequency between users' gender and their response (action).

Table 33: Frequencies gender

			Action		Total
			Victim	Detector	
Gender	Male	Count	53	92	145
		Expected Count	56.6	88.4	145.0
	Female	Count	20	22	42
		Expected Count	16.4	25.6	42.0
Total		Count	73	114	187
		Expected Count	73.0	114.0	187.0

Table 34: Chi-square test gender

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.676	1	.195		
Continuity Correctionb	1.243	1	.265		
Likelihood Ratio	1.652	1	.199		
Fisher's Exact Test				.212	.133
Linear-by-Linear Association	1.667	1	.197		
N of Valid Cases	187				

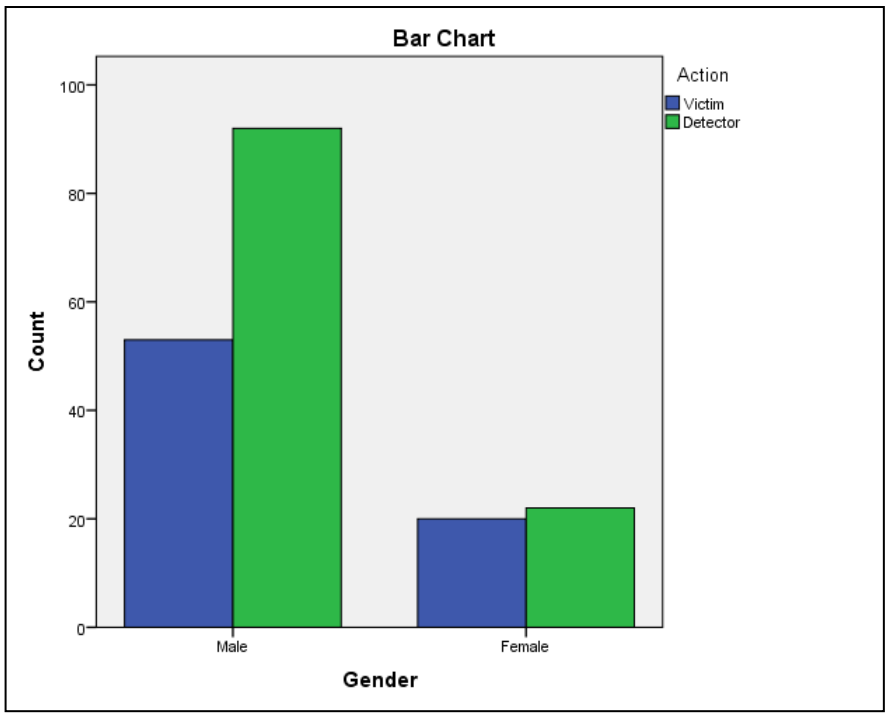

Figure 25: Frequencies chart gender

5.3.3 Culture

As noted above, the Australian study (but not the Saudi Arabian study) showed variance between users in relation to cultural background. The culture variables were measured with two items (language and nationality) and tested with users' response to the phishing email. The results are shown below.

5.3.3.1 Language

In the Australian study, the majority of participants (57%) reported that their first language is English (see Table 35), which enhances the ability to spot phishing email cues. Previous studies have reported that users are able to detect phishing emails through grammatical or spelling mistakes in their content (Jakobsson et al., 2007). Our results using the Chi-square test showed that users whose first language is not English have significantly increased vulnerability to phishing emails (see Table 36). Figure 26 shows the frequency between users' first language and users' response to phishing emails (action).

Table 35: Frequencies language

			Action		Total
			Victim	Detector	
Language	English	Count	24	83	107
		Expected Count	41.8	65.2	107.0
	Not English	Count	49	31	80
		Expected Count	31.2	48.8	80.0
Total		Count	73	114	187
		Expected Count	73.0	114.0	187.0

Table 36: Chi-square test language

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	28.987	1	.000		
Continuity Correctionb	27.379	1	.000		
Likelihood Ratio	29.444	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	28.832	1	.000		
N of Valid Cases	187				

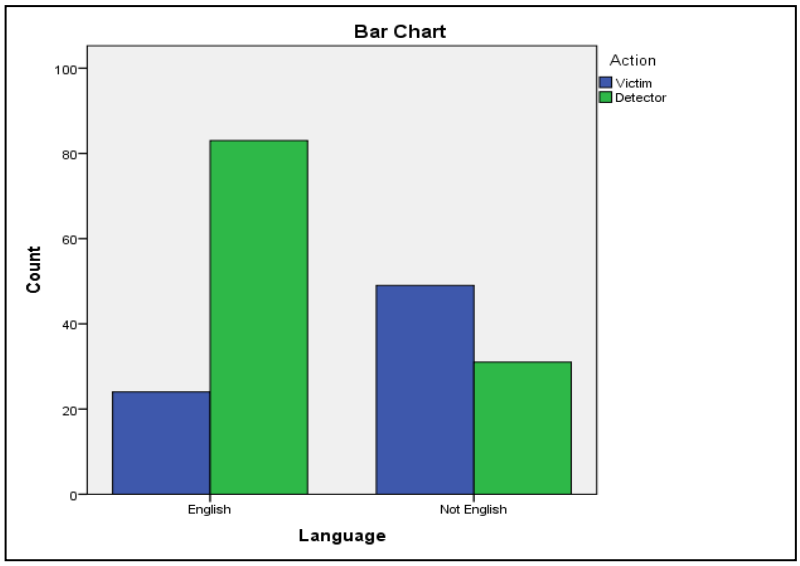

Figure 26: Frequencies chart language

5.3.3.2 Nationality

The majority (58%) of participants in the Australian study reported their nationality as Australian (see Table 37). Analysis using a Chi-square test showed that users' whose nationality differs from that of the impersonated entity have significantly increased vulnerability to phishing emails (see Table 38). Australian participants were more able to detect phishing emails that impersonated organisations in their country.

This is consistent with the findings from deception studies generally. Users found it hard to detect deception across cultures if the deception was conducted in a poor medium (Bond et al., 1990). Email is a poor medium, which increases the difficulty for users from a different culture to spot cues of deception.

The results on language and nationality show that users who come from a culture other than that from which phishing emails are generated are more vulnerable than users who come from the same culture. In our study, it should be noted, such participants are students who may only have lived in Australia for a couple of years and therefore may not have sufficient knowledge of the language or organisational policy to detect phishing emails that impersonate Australian organisations and use Australian (English) language. These findings may not apply to users who come

from a different culture but have been here long enough to be familiar with Australian culture. Further investigation is needed. Figure 27 shows frequency in relation to users' nationality and their response (action).

Table 37: Frequancy nationality

			Action		Total
			Victim	Detector	
Nationality	Australian	Count	28	81	109
		Expected Count	42.6	66.4	109.0
	Not Australian	Count	45	33	78
		Expected Count	30.4	47.6	78.0
	Total	Count	73	114	187
		Expected Count	73.0	114.0	187.0

Table 38: Chi-square test nationality

	Value	df	Asymp. Sig. (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	19.568	1	.000		
Continuity Correctionb	18.246	1	.000		
Likelihood Ratio	19.687	1	.000		
Fisher's Exact Test				.000	.000
Linear-by-Linear Association	19.464	1	.000		
N of Valid Cases	187				

Additionally, our study provides the opportunity to compare users from two cultures who receive phishing emails generated in their own culture. The comparison between two different cultures (Saudi Arabia and Australia) shows that culture does impact users' ability to detect. The Saudi Arabian study has fewer victims than the Australian study. This finding, however, does not suggest that Saudi Arabian users are better detectors than Australian users. Several other factors have an impact on users' detection. These are discussed in more detail in Section 7.2.

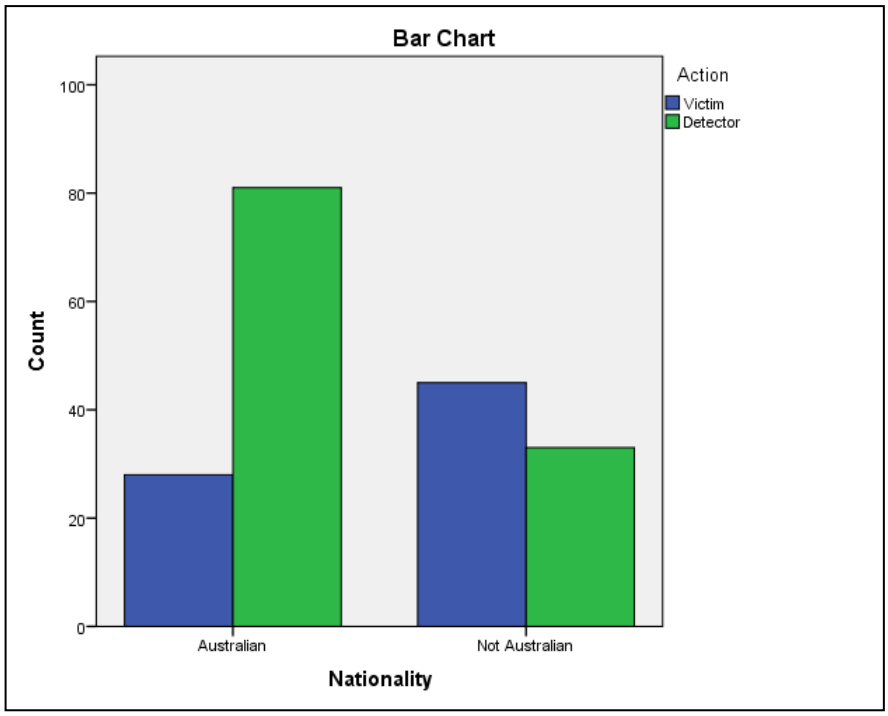

Figure 27: Frequency chart nationality

5.3.4 Usage

Spearman's test measures the correlation between two variables. This measure shows a significant correlation between the five items measuring users' usage with their response to phishing emails (Table 39). The findings show that years using the Internet (rho= -0.290, p<0.001), years using the email service (rho= -0.326, p<0.001), and years using the university email service (rho=-0.208, p<0.01), have a significant negative correlation with users' response to phishing emails. This means that when these three items increase, the likelihood of users responding to phishing emails decreases.

In contrast, number of hours using the Internet (rho=0.243, p<0.001) and number of emails received per day (rho=0.217, p<0.01) has a significant positive correlation with users' response to phishing emails. This means that when these two items increase, users' likelihood of responding to phishing emails increases. An explanation is that these users are heavy users. Spending much time in the Internet and receiving high number of emails limit these users ability to make a rigours and reasonable decision about phishing email. Since, those users need to make dictions to high number of emails. Vishwanath et al. (2011) found a similar result which is high number of received emails increase users being victims to phishing emails. These

results are from the Australian study. The Saudi Arabian study did not show any significant correlation between variables which might have contributed to the low number of victims (14) in the Saudi Arabian study.

Table 39: Spearman's rho test with usage (Australia)

		Response	Y_Internet	H_Internet	Y_Email	Y_Uni	No_Email
Response	Correlation Coefficient	1.000	-.290**	.243**	-.326**	-.208**	.217**
	Sig. (1-tailed)	.	.000	.000	.000	.002	.001
	N	187	187	187	187	187	187
Y_Internet	Correlation Coefficient	-.290**	1.000	-.138*	.707**	.100	-.168*
	Sig. (1-tailed)	.000	.	.030	.000	.086	.011
	N	187	187	187	187	187	187
H_Internet	Correlation Coefficient	.243**	-.138*	1.000	-.170**	-.046	.046
	Sig. (1-tailed)	.000	.030	.	.010	.264	.268
	N	187	187	187	187	187	187
Y_Email	Correlation Coefficient	-.326**	.707**	-.170**	1.000	.145*	-.207**
	Sig. (1-tailed)	.000	.000	.010	.	.024	.002
	N	187	187	187	187	187	187
Y_Uni	Correlation Coefficient	-.208**	.100	-.046	.145*	1.000	-.094
	Sig. (1-tailed)	.002	.086	.264	.024	.	.101
	N	187	187	187	187	187	187
No_Email	Correlation Coefficient	.217**	-.168*	.046	-.207**	-.094	1.000
	Sig. (1-tailed)	.001	.011	.268	.002	.101	.
	N	187	187	187	187	187	187

5.3.5 Internet activities

Spearman's test measures the correlation between two variables. This measure shows a significant correlation between the three items measuring Internet activities with users' response to phishing emails (Table 40). The findings show that shopping (rho= -0.183, $p<0.01$) has a significant negative correlation with users' response to phishing emails. This means that when this item increases, the likelihood of users responding to phishing emails decreases. In contrast, surfing the Internet (rho=0.131, $p<0.05$) has a significant positive correlation with users' response to phishing emails. This means that when this item increases, users' likelihood of responding to phishing emails increases. This is consistent with the findings from Wright et al (2009). People use the Internet for different purposes, such as communicating with friends or reading newspapers, or for shopping or banking, which require knowledge of

technical security. Our study found that conducting sensitive transactions in the Internet influences users' security perceptions and behaviour. These results only relate to the Australian study. The Saudi Arabian study did not show any significant correlation between variables, which might reflect the way in which the question was asked (see Section 4.5.11) as well as the low number (14) of victims in the Saudi Arabian study.

Table 40: Spearman's rho test with Internet Activities (Australia)

		Response	Surfing	Social	Shopping
Response	**Correlation Coefficient**	1.000	.131*	.101	-.183**
	Sig. (1-tailed)	.	.037	.085	.006
	N	187	187	187	187
Surfing	**Correlation Coefficient**	.131*	1.000	.232**	.163*
	Sig. (1-tailed)	.037	.	.001	.013
	N	187	187	187	187
Social	**Correlation Coefficient**	.101	.232**	1.000	.078
	Sig. (1-tailed)	.085	.001	.	.145
	N	187	187	187	187
Shopping	**Correlation Coefficient**	-.183**	.163*	.078	1.000
	Sig. (1-tailed)	.006	.013	.145	.
	N	187	187	187	187

5.4 Instrument Validation

This section describes the processes we used to measure instrument reliability and factor analysis to test uni-dimensionality and validity of variables.

5.4.1 Reliability

Reliability measures the internal consistency between items to measure constructs. The reliability measure concerns consistency and stability of a measure (Sekaran, 2003).

Table 41 presents the values obtained from conducting a reliability test using SPSS. Cronbach's alpha was used to measure reliability in each construct. Scholars

suggests that Cronbach's alpha of 0.7 is the acceptable cut-off value (Hair, Black, Babin, Anderson, & Tatham, 2010).

Table 41: Reliability measure

	Saudi Arabia		Australia	
Variables	**Alpha**	**Items**	**Alpha**	**Items**
Trust	.395	3	.864	3
Submissiveness	.894	16	.981	16
Email experience	.872	6	.910	6
Email richness	.743	4	.925	4
Susceptibility	.775	5	.932	3

In both studies, almost all the constructs included in our research complied with the requirements of the reliability measure, with one exception—the trust variable in the Saudi Arabian study. Therefore, the trust variable in the Saudi Arabian study was omitted from further analysis.

5.4.2 Variables validity

Variables validity and uni-dimensionality were measured using exploratory factor analysis (EFA). Variables validity was also measured by obtaining convergent validity as well as discriminate validity which were conducted using confirmatory factor analysis (CFA).

5.4.2.1 Exploratory factor analysis (EFA)

Exploratory factor analysis is a useful technique which can be used to understand a set of constructs (Field, 2009). Principal component factor analysis with varimax rotation was used in the measurement for each reliable construct in the survey. The measurement was conducted using SPSS version 21. The pilot study did not have sufficient participants to conduct EFA, in addition to the existence of latent variables, so our research included factor analysis in this stage. The extraction method called "fixed number of factors" is used to force the measurement under four factors for the Saudi Arabian study (trust is omitted) and five factors for the

Australian study. The number of factors forced in these two studies is limited to the number of satisfied latent variables achieved by Cronbach's alpha test. The results for both Saudi Arabian and Australian studies are shown in Table 42 and Table 43 respectively.

Table 42: Exploratory factor analysis (Saudi Arabia)

	1	2	3	4
Email_Exp1	**0.811**	0.023	-0.193	0.259
Email_Exp2	**0.755**	-0.045	-0.161	0.285
Email_Exp3	**0.739**	-0.073	-0.126	0.326
Email_Exp4	**0.736**	0.048	-0.136	0.213
Email_Exp5	**0.736**	0.063	0.021	-0.127
Email_Exp6	**0.439**	0.222	0.212	-0.349
Email_rich1	**0.653**	0.041	0.133	-0.096
Email_rich2	**0.645**	-0.011	0.144	-0.102
Email_rich3	**0.58**	-0.157	0.167	-0.222
Email_rich4	**0.69**	-0.078	0.074	-0.031
Missive1	0.186	**0.541**	0.111	-0.059
Missive2	-0.247	**0.611**	0.033	0.003
Missive3	-0.07	0.232	0.069	**0.458**
Missive4	-0.005	**0.624**	0.158	-0.082
Missive5	0.07	**0.612**	-0.039	-0.005
Missive6	0.023	-0.055	0.26	**0.556**
Missive7	0.039	0.117	-0.017	**0.299**
Missive8	0.075	**0.497**	0.116	-0.254
Missive9	-0.082	0.317	0.131	**0.505**
Missive10	0.123	**0.517**	0.147	0.278
Missive11	-0.082	0.26	-0.143	**0.342**
Missive12	0.079	-0.06	0.064	**0.525**
Missive13	0.011	0.155	-0.102	**0.614**
Missive14	-0.096	**0.658**	-0.215	0.022
Missive15	-0.121	0.241	0.153	**0.462**
Missive16	-0.098	**0.442**	0.375	-0.32
Bank	0.191	0.097	**0.599**	0.159
eBay	0.034	-0.049	**0.806**	0.023
PayPal	-0.094	0.099	**0.735**	0.005
Scam	-0.176	0.143	0.206	**0.483**
Uni	-0.017	-0.011	0.385	**0.513**

In the Saudi Arabian study, exploratory factor analysis showed that some items had weak loadings on their expected factor. As a result these items were removed from their expected factors. Only those items with a load high on their expected factors were retained. In addition, perceived email experience and email richness items have high loading as one factor (Table 42). This means that these 10 items

measure the same construct. Therefore, one of the factors was removed; we chose to remove perceived email experience because either factor will give the same results.

Table 43: Exploratory factor analysis (Australia)

	1	2	3	4	5
Trust1	-0.175	-0.534	**0.526**	-0.19	0.345
Trust2	-0.232	-0.418	**0.559**	-0.222	0.369
Trust3	-0.239	-0.343	**0.613**	-0.258	0.32
Email_Exp1	0.245	**0.721**	-0.176	0.2	-0.071
Email_Exp2	0.383	**0.701**	-0.335	0.003	0.267
Email_Exp3	0.347	**0.701**	-0.316	0.027	-0.058
Email_Exp4	0.268	**0.613**	-0.316	0.066	0.19
Email_Exp5	0.376	**0.683**	-0.264	0.128	-0.078
Email_Exp6	-0.075	**0.632**	0.149	-0.329	0.259
Email_rich1	0.356	0.265	0.29	**0.717**	-0.046
Email_rich2	0.358	0.24	0.371	**0.734**	0.094
Email_rich3	0.302	0.141	0.371	**0.642**	0.16
Email_rich4	0.235	0.187	0.34	**0.632**	0.291
Missive1	**0.897**	-0.013	0.15	0.078	0.028
Missive2	**0.884**	0.025	0.236	0.023	-0.003
Missive3	**0.857**	0.066	0.144	-0.001	-0.001
Missive4	**0.912**	-0.026	0.119	-0.022	0.003
Missive5	**0.747**	0.223	0.278	-0.079	-0.162
Missive6	**0.835**	0.145	0.322	-0.055	-0.022
Missive7	**0.811**	0.171	0.209	0.052	-0.024
Missive8	**0.856**	0.174	0.155	-0.141	0.094
Missive9	**0.867**	0.077	0.221	0.022	-0.124
Missive10	**0.882**	0.153	0.163	-0.068	0.07
Missive11	**0.884**	-0.047	0.134	-0.02	-0.109
Missive12	**0.802**	0.17	0.213	-0.007	0.138
Missive13	**0.897**	-0.015	0.075	-0.008	-0.048
Missive14	**0.887**	0.021	0.173	-0.056	0.015
Missive15	**0.874**	-0.073	0.153	0.022	-0.16
Missive16	**0.857**	-0.064	0.205	-0.015	-0.041
Bank	0.195	-0.495	0.225	-0.184	**0.599**
eBay	0.259	-0.444	0.229	-0.133	**0.69**
PayPal	0.285	-0.366	0.038	-0.179	**0.756**
Scam	0.231	-0.082	0.15	-0.108	**0.844**
Uni	0.237	-0.206	0.031	-0.198	**0.815**

EFA result in finding four constructs in Saudi Arabian study and five constructs in Australian study (see Table 42 and Table 43). In Saudi Arabia, 4 items

used to measure email richness. 8 items out of 16 items used to measure submissiveness. 3 items used to measure susceptibility. Items loaded high outside their expected constructs were omitted. In Australian study, 3 items used to measure trust. 4 items used to measure email richness. 16 items used to measure submissiveness. 6 items used to measure email experience. 5 items used to measure susceptibility. It can be seen from these two tables that there are some items loaded weak in their expected construct in Saudi Arabia (see Table 42) not like the results obtained in Australia (see Table 43). An explanation for these differences can be attributed to biased answers given by Arab participants (Baron-Epel, Kaplan, Weinstein, & Green, 2010; Smith, 2004). Arab participants have been found to give more positive or extreme answers to attitude questions. Most of our items ask about attitudes which indicate that Arab participants gave biased answers. In our research, items used to measure constructs are obtained from validated studies. The survey was piloted twice and the translation followed back translation with translation service experts.

5.4.2.2 Confirmatory factor analysis (CFA)

Confirmatory factor analysis is used to examine construct validity for all the valid variables used in our research. CFA also has a strong relationship with structure equation modelling (SEM). CFA cannot be employed using SPSS. Therefore, partial least Square (SmartPLS 2.0) was used to conduct CFA.

Table 44 shows that the minimum requirement for factor loading above 0.4 is met by the items in the survey. All items have loaded on their expected factor. Average variance extracted (AVE) for each construct met the minimum requirement of 0.5 and above, as suggested by Fornell and Larcker (1981). Results shown in Table 44, Table 45, Table 46 and Table 47 support the conclusion that convergent validity is obtained among constructs in both studies.

Discriminant validity was also tested using a suggestion made by Anderson and Gerbing (1960). The test suggests that discriminant validity can be obtained by comparing the average variance extracted (AVE) for each variable and the square correlation between a pair of latent variables. AVE (bolded numbers in tables: 44 and 46) should be greater than the square correlation between a pair of latent variables.

Table 45 and Table 47 show that this requirement has been satisfied in both studies. It can be concluded that discriminant validity has been obtained for the constructs used in our research.

Table 44: Factor loading (Saudi Arabia)

	Email richness	Submissiveness	Susceptibility
Email_rich1	**0.9592**	-0.0869	0.2675
Email_rich2	**0.9648**	-0.1110	0.3354
Email_rich3	**0.9719**	-0.1877	0.2559
Email_rich4	**0.9662**	-0.0918	0.2656
Missive1	-0.1079	**0.7749**	0.1430
Missive10	-0.0457	**0.7702**	0.0902
Missive14	-0.1285	**0.8029**	0.1130
Missive16	-0.1489	**0.8340**	0.1611
Missive2	-0.0098	**0.8321**	0.0932
Missive4	-0.1483	**0.8802**	0.0886
Missive5	-0.0873	**0.7605**	0.0969
Missive8	-0.1324	**0.8409**	0.0913
Bank	0.2666	0.1268	**0.8522**
PayPal	0.1624	0.0976	**0.7128**
eBay	0.1758	0.0859	**0.7399**

Table 45: Discriminate validity (Saudi Arabia)

	Email richness	Submissiveness	Susceptibility
Email richness	**0.578**		
Submissiveness	0.006512	**0.6695**	
Susceptibility	0.003856	0.019612	**0.6365**

Table 46: Factor loading (Australia)

	Email experience	Email richness	Submissiveness	Susceptibility	Trust
Trust1	-0.0744	-0.356	0.3491	0.5362	**0.8546**
Trust2	0.0836	-0.4585	0.4729	0.5235	**0.8922**
Trust3	0.1746	-0.4713	0.5307	0.4353	**0.913**
Email_Exp1	**0.8374**	-0.1643	0.4357	0.1728	0.0653
Email_Exp2	**0.8696**	-0.2217	0.3469	0.1562	-0.029
Email_Exp3	**0.8892**	-0.2705	0.4142	0.1748	0.0497
Email_Exp4	**0.8804**	-0.2598	0.4295	0.2607	0.0878
Email_Exp5	**0.8785**	-0.2364	0.4484	0.2306	0.0728
Email_Exp6	**0.6868**	0.1162	0.0796	-0.0875	-0.103
Email_rich1	-0.2307	**0.9064**	-0.6321	-0.6741	-0.477
Email_rich2	-0.2803	**0.949**	-0.6359	-0.6747	-0.511
Email_rich3	-0.3123	**0.8907**	-0.5559	-0.5424	-0.355
Email_rich4	-0.2424	**0.871**	-0.547	-0.5519	-0.396

Missive1	0.419	-0.5904	**0.9071**	0.342	0.534
Missive10	0.5259	-0.5954	**0.9031**	0.4496	0.3992
Missive11	0.3878	-0.4379	**0.8937**	0.5099	0.5317
Missive12	0.494	-0.4863	**0.8341**	0.5768	0.3585
Missive13	0.422	-0.5654	**0.8976**	0.4299	0.517
Missive14	0.4214	-0.6312	**0.9086**	0.3833	0.4528
Missive15	0.3484	-0.6213	**0.8847**	0.4107	0.541
Missive16	0.3472	-0.595	**0.8788**	0.5877	0.4923
Missive2	0.4178	-0.5659	**0.9154**	0.3735	0.4932
Missive3	0.4668	-0.5697	**0.871**	0.5648	0.4613
Missive4	0.421	-0.656	**0.9164**	0.4385	0.5388
Missive5	0.4699	-0.4521	**0.7926**	0.4803	0.2803
Missive6	0.4446	-0.5001	**0.8861**	0.591	0.3457
Missive7	0.479	-0.4936	**0.8395**	0.5872	0.3862
Missive8	0.5285	-0.602	**0.8775**	0.3182	0.3463
Missive9	0.452	-0.5614	**0.8977**	0.5353	0.4636
Bank	0.0524	-0.5077	0.5087	**0.8273**	0.3376
eBay	0.1014	-0.546	0.4055	**0.9032**	0.4493
PayPal	0.2098	-0.6594	0.5668	**0.9135**	0.5049
Scam	0.4064	-0.6072	0.384	**0.884**	0.5553
Uni	0.3369	-0.6858	0.5323	**0.9053**	0.5694

Table 47: Discriminate validity (Australia)

	Email experience	**Email richness**	**Submissiveness**	**Susceptibility**	**Trust**
Email experience	**0.753**				
Email richness	0.07177	**0.8187**			
Submissiveness	0.256441	0.395641	**0.7753**		
Susceptibility	0.015826	0.389251	0.374789	**0.8429**	
Trust	0.004733	0.234159	0.216783	0.47087	**0.787**

5.5 Hypothesis Testing

This section presents the results obtained from hypothesis testing and the structural model. Since our research has a categorical dependent variable (response), logistic regression was employed to test the hypothesis with a binary categorical variable. R software with Lavaan packages was employed to test the overall model (Rosseel, 2012). Lavaan packages have been proposed to test SEM models which include categorical variables as dependent variables (Rosseel, 2013).

Since our research has two dependent variables (susceptibility and response), multiple linear regression was used to test the hypothesis regarding the susceptibility variable, and logistic regression was employed to test the hypothesis regarding the

response variable. The final model was tested with R software which has the ability to test SEM that includes a categorical variable as a dependent variable (i.e. response), unlike AMOS or SmartPLS. The analysis is organised to show results from the Saudi Arabian study first, because this study was conducted first and its data were analysed before the Australian study was implemented.

5.5.1 Justification for using regression

At the beginning of the analysis we applied linear and logistic regression. The advantage of linear regression is its ability to test the regression coefficient (Beta value) *individually* between variables, and the advantage of logistic regression is its ability to test the regression coefficient on a binary categorical dependent variable which is not typical for SEM. One drawback of linear and logistic regressions is that they are limited to measuring only one dependent variable. Since our research has two dependant variables, the overall model is measured using SEM.

5.5.2 Hypothesis testing using regression

We were interested in investigating the impact of unique variables on their dependent variable, which can be achieved by regression. Regression was applied by conducting several linear regressions with the susceptibility variable and several logistic regressions with the response variable. The hypothesis testing involves investigating the impact of various predictors on a singular dependent variable (Hair et al., 2010).

5.5.2.1 Regression analysis steps

This section explains the three main analytical steps used to test our research hypotheses. These are:

1. Factors are presented by their scores which are obtained from computing the average scores for the items in each factor.
2. Testing predictors individually with their related dependent variable.
3. Applying the regression and interpreting the results.

5.5.2.2 Factor score

This step is applied to enable us to conduct the regression analysis. The factor score was calculated by computing the score for every item presenting the factor (Comrey & Lee, 2013). Then, the score was divided by the number of items to maintain the scale metric. For example, email richness is measured with 4 items. Therefore, the final score was calculated as follows:

Email richness = (Email_rich1 + Email_rich2 + Email_rich3 + Email_rich4)/ 4.

5.5.2.3 Regression analysis

The regression coefficient value is used for comparison and to help test the relationship between variables used in the regression model. The importance and strength of the relationship can be obtained by examining the value of the coefficient. The relationship between independent variables and dependent variables can be positive or negative. The significance of the relation can be obtained when the value of "p" is less than 0.05 (Field, 2009).

5.5.2.4 Testing the relationship between variables individually

The first step in regression was to test the impact of each independent variable with its related dependent variable (susceptibility and response). Only those independent variables that have a significant relationship with the dependent variable were grouped together and entered into the final model. This procedure allows us to prevent insignificant variables from entering the final model. The results of this procedure are explained below (see Table 48, Table 49, Table 50 and Table 51). Since submissiveness was significant in the Saudi Arabian study, in the Australian study it was entered first with susceptibility, along with susceptibility and openness with response (see Table 50 and Table 51). These tables' summaries the results obtained from these tests. For more information please see the following section.

Table 48: Linear regression with susceptibility as a dependent variable (Saudi Arabia)

Independent variables	Test results
Submissiveness	There is a positive and significant relationship between submissiveness and users' susceptibility

Table 49: Logistic regression with response as a dependent variable (Saudi Arabia)

Independent variables	Test results
Susceptibility	There is a positive and significant relationship between susceptibility and users responding to phishing emails
Openness	There is a positive and significant relationship between openness and users responding to phishing emails

Table 50: Linear regression with susceptibility as a dependent variable (Australia)

Independent variables	Test results
Submissiveness	There is a positive and significant relationship between submissiveness and users' susceptibility
Trust	There is a positive and significant relationship between trust and users' susceptibility
Perceived Email Richness	There is a negative and significant relationship between email richness and users' susceptibility
Extraversion	There is a positive and significant relationship between extraversion and users' susceptibility
Agreeableness	There is a positive and significant relationship between agreeableness and users' susceptibility
Conscientiousness	There is a positive and significant relationship between conscientiousness and users' susceptibility
Emotional Stability	There is a negative and significant relationship between emotional stability and users' susceptibility
Openness	There is a positive and significant relationship between openness and users' susceptibility

Table 51: Logistic regression with response as a dependent variable (Australia)

Independent variables	Test results
Susceptibility	There is a positive and significant relationship between susceptibility and users responding to phishing emails
Openness	There is a positive and significant relationship between openness and users responding to phishing emails
Trust	There is a positive and significant relationship between trust and users responding to phishing emails
Email Richness	There is a negative and significant relationship between email richness and users responding to phishing emails
Extraversion	There is a positive and significant relationship between extraversion and users responding to phishing emails
Agreeableness	There is a positive and significant relationship between agreeableness and users responding to phishing emails
Conscientiousness	There is a positive and significant relationship between conscientiousness and users responding to phishing emails
Emotional Stability	There is a negative and significant relationship between emotional stability and users responding to phishing emails
Confirmation	There is a negative and significant relationship between the type of confirmation channel and users responding to phishing emails

5.5.2.5 Applying the regression and interpreting the results

This section describes the results obtained from testing only significant independent variables with dependent variables (susceptibility and response).

Susceptibility as an outcome

The major hypothesis is that predictor variables have an impact on users' susceptibility (i.e., likelihood that he/she would not suspect a phishing email). In the

beginning, we need to satisfy the assumptions of linear regression. The results obtained are presented below:

Linearity and homoscedasticity

Linearity can be examined from the scatter plot (see Figure 28 and Figure 29). As can be seen, residuals did not show any nonlinear pattern (Hair et al., 2010). The data points in the scatter are random. We can conclude from this result that linearity and homoscedasticity are satisfied.

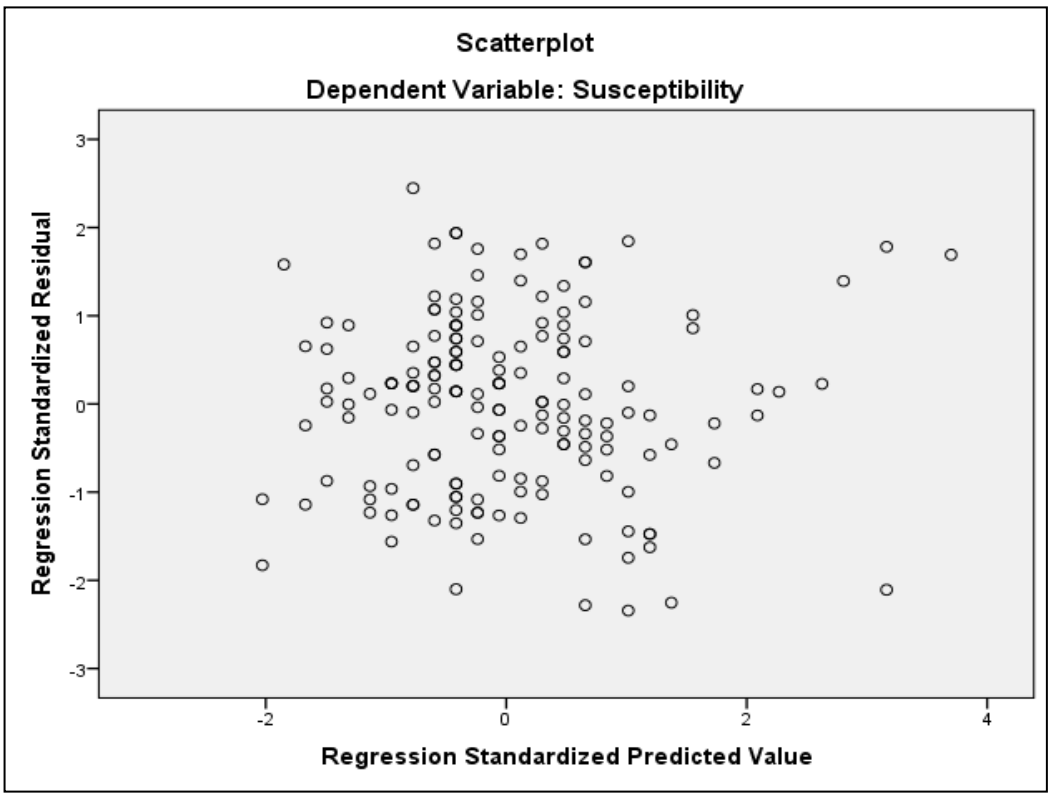

Figure 28: Regression scatter plot (Saudi Arabia)

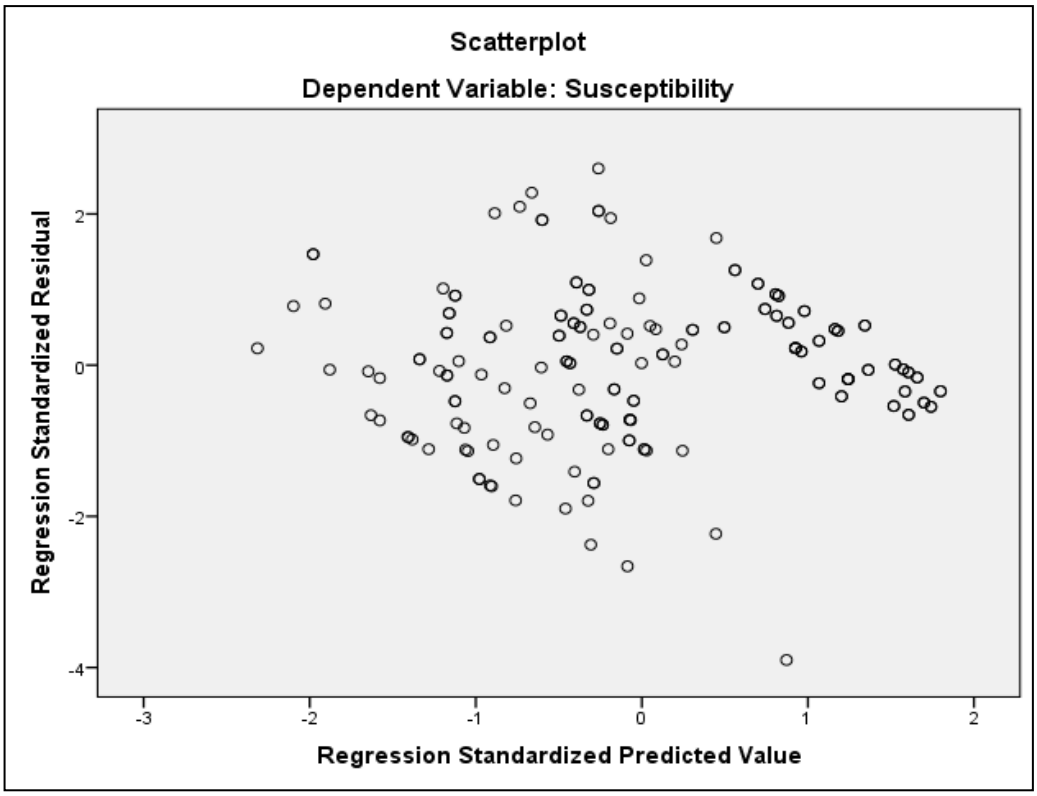

Figure 29: Regression scatter plot (Australia)

Normality

Normality can be examined by looking at the values provided by skewness and kurtosis. The normal distribution of the data is close to zero of these two measures (Field, 2009; Hair et al., 2010). In addition, some scholars suggest that normality can be assumed by having a large number sample size (e.g. more than 40 cases) (Field, 2009). In both our studies, the number of participants exceeded 100 cases, which satisfies the normality requirement.

Multicollinearity

Multicollinearity measures the relationship between the predictors and suggests that these predictors have a strong relationship (Hair et al., 2010). There are two measures to satisfy this requirement: variable inflation factor (VIF), which should be below 10, and tolerance level (TOL), which should be above 0.1 to conclude the absence of multicollinearity (Field, 2009; Hair et al., 2010). In the Saudi Arabian study, this test was not required (i.e. multicollinearity) since the regression test only

had one independent variable. For the Australian study, Table 52 shows that predictors examined in our research are suitable for conducting multiple regressions.

Table 52: Collinearity statistics

Predictors	Collinearity Statistics	
	Tolerance	VIF
Submissiveness	.374	2.671
Trust	.481	2.081
Email Richness	.391	2.558
Extraversion	.447	2.236
Agreeable	.819	1.221
Conscientious	.672	1.487
Emotional Stable	.623	1.605
Openness	.589	1.698

Independence of residuals

The Durbin-Watson test can be used to test the dependency of residuals. Durbin-Watson measures the correlations between residuals. If the result obtained from the Durbin-Watson test is close to 2, this means that there is an independency between residuals (Field, 2009). This measure has been satisfied in both studies. The values obtained from the Durbin-Watson test are 1.938 and 1.812 for the Saudi Arabian and Australian studies, respectively, both of which are very close to 2. Therefore, it can be concluded that the independence of residuals is satisfied.

Outliers

The Cook distance measured with the regression shows that the outliers' values do not influence the regression model. The values obtained from the Cook Distance test range between 0.000 and 0.166 and 0.000 and 0.170 in the Saudi Arabian and Australian studies, respectively, which is an acceptable result. Values greater than 1 would raise concern about the results (Field, 2009). Having satisfied the assumptions for linear regression, we discuss the results below. The Saudi Arabian results are presented first.

Saudi Arabian results from linear regression (Table 53 and Table 54) show that there is a positive significant relationship between submissiveness and susceptibility. Submissiveness explains 3% of the variance in susceptibility. The overall model

shows a significant impact on susceptibility caused by the proposed model ($p < 0.05$) (see Table 53).

Table 53 shows that the standardised coefficient (Beta value) for submissiveness is 0.167 and the relationship between submissiveness and susceptibility is positive.

Table 53: Linear regression result – susceptibility (Saudi Arabia)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.122	.372		8.402	.000
	Submissiveness	.323	.148	.167	2.188	.030

Table 54: Model summary – susceptibility (Saudi Arabia)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.167	.028	.022	1.3371

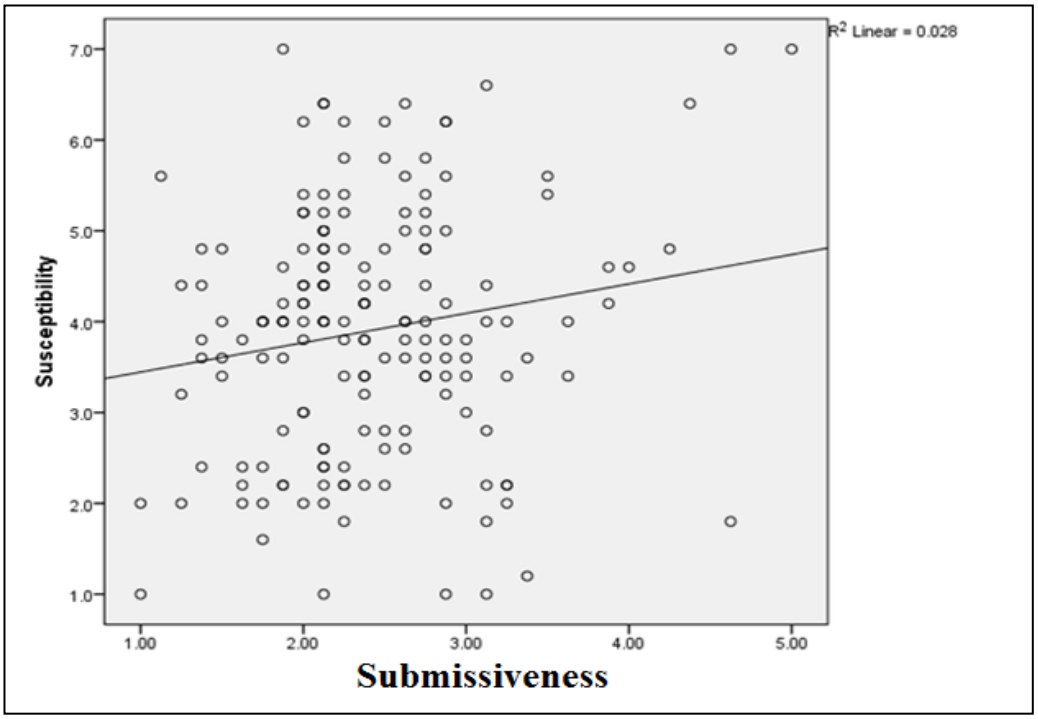

Figure 30: Scatter plot with submissiveness mean scores on X axis and susceptibility mean scores on the Y axis

As shown in Figure 30, participants with a higher mean score for submissiveness also had higher mean scores for susceptibility. The flaring out of confidence intervals is consistent with less-than-perfect fit at the extremes of low and high scores.

Australian results from multiple regressions (Table 55 and Table 56) show that there are two positive significant relationships between submissiveness and trust with susceptibility being the dependent variable. There is also a negative and significant relationship between perceived email richness and susceptibility. The results show that submissiveness, trust and email richness explain 64% of the variance in susceptibility. The overall model shows a significant impact on susceptibility caused by the proposed model ($p < 0.001$) (see Table 55).

Table 55 shows that the standardised coefficients (Beta value) are 0.190 for submissiveness, 0.475 for trust and -0.199 for email richness. There is a positive relationship between submissiveness and trust, and susceptibility. In contrast, there is a negative relationship between email richness and susceptibility.

Table 55: Linear regression result – susceptibility (Australia)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.870	1.343		1.392	.166
	Submissiveness	.188	.074	.190	2.542	**.012**
	Trust	.546	.076	.475	7.208	**.000**
	Email_Rich	-.210	.077	-.199	-2.724	**.007**
	Extraversion	.048	.067	.050	.727	.468
	Agreeableness	.108	.109	.050	.999	.319
	Conscientiousness	.009	.079	.006	.114	.909
	Emotional	-.094	.080	-.068	-1.174	.242
	Openness	-.125	.090	-.083	-1.389	.167

Table 56: Model summary – susceptibility (Australia)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.802	.643	.616	1.19161

Response as an outcome

A major hypothesis is that predictor variables have an impact on users' response (i.e., likelihood that he/she would respond to a phishing email). Initially, we needed to satisfy logistic regression assumptions. The main assumptions for logistic regression are binary categorical dependent variable and sample size above 50 (Hutcheson, 1999). These two assumptions are satisfied in our study. The dependent variable response is a binary category (detectors or victims) and the sample size is large enough for the conduct of logistic regression. The sample sizes are 196 and 187 in the Saudi Arabian and Australian studies, respectively. Having satisfied these assumptions, we present the results obtained from logistic regression below. The Saudi Arabian data are examined first.

In the Saudi Arabian study (Table 57), both predictors, openness and susceptibility, were significant at the $p < 0.05$ level. These variables increase users' response to phishing emails.

Based on the Cox & Snell R-square (see Table 58), this model explained 6% of the variance, with the Omnibus model of coefficients statistically significant at the $p < 0.01$ level, which is consistent with this model explaining a significant percentage of the variance. Both openness and susceptibility have a positive and significant relationship with response.

Table 57: Final logistic regression model with response as outcome (Saudi Arabia)

	B	S.E.	Wald	df	Sig.	Exp(B)
Susceptibility	.465	.203	5.221	1	.022	1.592
Openness	.588	.255	5.307	1	.021	1.801
Constant	-7.700	1.725	19.922	1	.000	.000

Table 58: Model summary – response (Saudi Arabia)

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	88.088	.063	.157

As indicated in Table 57, both susceptibility and openness predicted response as an outcome at the $p < 0.05$ level. Those with higher openness and susceptibility

scores were two times more likely than others (Exp (B)) to respond to the phishing emails.

In Australia, Table 59 shows that both predictors, openness and susceptibility, were significant at the $p < 0.01$ level. These variables increase users' response to phishing emails. This result supports the findings from the Saudi Arabian study. In addition to other predictors that are significant included extraversion, agreeableness and type of confirmation channel.

Based on the Cox & Snell R-square (see Table 59), this model explained 49% of the variance, with the Omnibus model of coefficients statistically significant at the $p < 0.001$ level, consistent with this model explaining a significant percentage of the variance. Susceptibility, openness, extraversion and agreeableness have a positive and significant relationship with response. Susceptibility and agreeableness are highly significant $p < 0.001$ and openness and extraversion are significant $p < 0.01$. The type of confirmation channel shows a negative and significant relationship. This means that rich confirmation channels are more likely to increase users' ability to detect phishing emails. Confirmation channel type shows a significant level with $p < 0.05$.

Table 59: Final logistic regression model with response as an outcome (Australia)

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1	**Susceptibility**	.914	.224	16.678	1	**.000**	2.495
	Openness	.859	.257	11.195	1	**.001**	2.360
	Extraversion	.540	.174	9.672	1	**.002**	1.716
	Agreeableness	1.289	.330	15.248	1	**.000**	3.631
	Conscientiousness	.246	.202	1.473	1	.225	1.278
	Emotional	.127	.200	.403	1	.526	1.135
	Trust	.039	.201	.037	1	.847	.962
	Email_Rich	-.359	.195	3.377	1	.066	1.432
	Channel	-.432	.200	4.643	1	**.031**	.649
	Constant	-16.920	3.786	19.973	1	.000	.000

Table 60: Model summary – response (Australia)

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	123.586	.492	.667

As indicated in Table 59, both susceptibility, openness, extraversion, agreeableness and confirmation channel predicted response as an outcome at the $p < 0.05$ level. Those with higher susceptibility and openness scores were two and half times more likely than others (Exp (B)) to respond to the phishing emails. Those with higher extraversion scores were two times more likely than others (Exp (B)) to respond to phishing emails. Those with higher agreeableness scores were four times more likely than others (Exp (B)) to respond to phishing emails. Those with higher confirmation channel scores were one time more likely than others (Exp (B)) to detect phishing emails. Table 61 shows the supported hypotheses obtained from regression in both studies.

Table 61: List of supported hypotheses

		Saudi Arabia		**Australia**	
No.	**Variables**	**Result**	**Supported**	**Result**	**Supported**
H1	Trust		N/A[9]	β = 0.475 and p = 0.000	Yes
H2	Submissiveness	β = 0.167 and p = 0.030	Yes	β = 0.190 and p = 0.012	Yes
H3	Perceived email experience		N/A		No
H4	Perceived email richness		No	*β = -0.199*[10] *and p = 0.007*	Yes
H5	Susceptibility	B = 0.465 and p = 0.022	Yes	B = 0.914 and p = 0.000	Yes
H6	Personality traits		No		No
H7	Personality traits Openness	B = 0.588 and p = 0.021	Yes	B = 0.859 and p = 0.001	Yes
	Extraversion		No	B = 0.540 and p = 0.002	Yes
	Agreeableness		No	B = 1.289 and p = 0.000	Yes
H8	Rich confirmation channel		No	*B = -0.432 and p = 0.031*	Yes

[9] N/A means that the hypothesis was not tested because the construct did not satisfy validity measurements
[10] Red indicates negative impact

5.5.3 Structural equation modelling (SEM)

SEM is suitable for analysing multiple dependent variables as well as multiple independent variables. One issue with SEM is the requirement for measuring the latent variable instead of the manifest variable. In our research, R software with Lavaan packages was used to analyse the overall model because of its ability to analyse SEMs with categorical dependent variables (Rosseel, 2013), unlike AMOS or SmartPLS. The results are explained below.

The measurement model has provided satisfactory reliability and validity. This means that the items used in our research have the ability to measure the construct they are expected to measure. The second step is to evaluate the research model using structural equation modelling (SEM). SEM is widely used as a test in behavioural studies (Baumgartner & Homburg, 1996).

Our research investigates users' behaviour when they are faced with phishing emails. Goodness of fit for the research model is explained in Figure 31 and Figure 32. Saudi Arabia and Australia have different values for the explained variance for response. The reason for this difference is discussed in Chapter 7. In Saudi Arabia, the overall model explains 13% of the variance responsible for users' behaviour (responding to phishing emails) (R^2= 0.126). In Australia, the overall model explains 45% of the variance responsible for users' behaviour (responding to phishing emails) (R^2= 0.45). Please the following tables for more details Table 62, Table 63, Table 64, and Table 65.

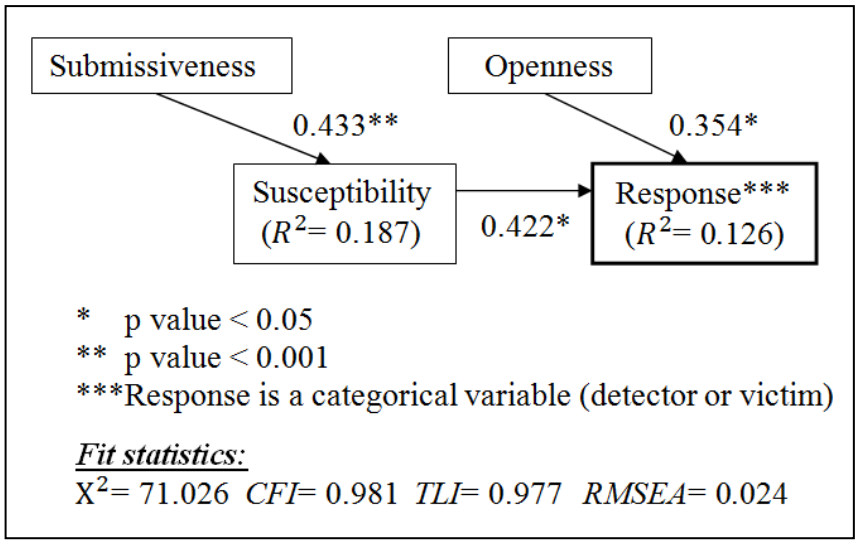

Figure 31: Structural model for Saudi Arabian study

Table 62: R Software results – Saudi Arabia

Path		Path coefficient	Standard error	P-value
ID	DV			
Submissiveness	Susceptibility	0.433	0.169	0.000
Susceptibility	Response	0.422	0.128	0.022
Openness	Response	0.354	0.157	0.038

Table 63: R square values – Saudi Arabia

	R square
Susceptibility	0.187
Response	0.126

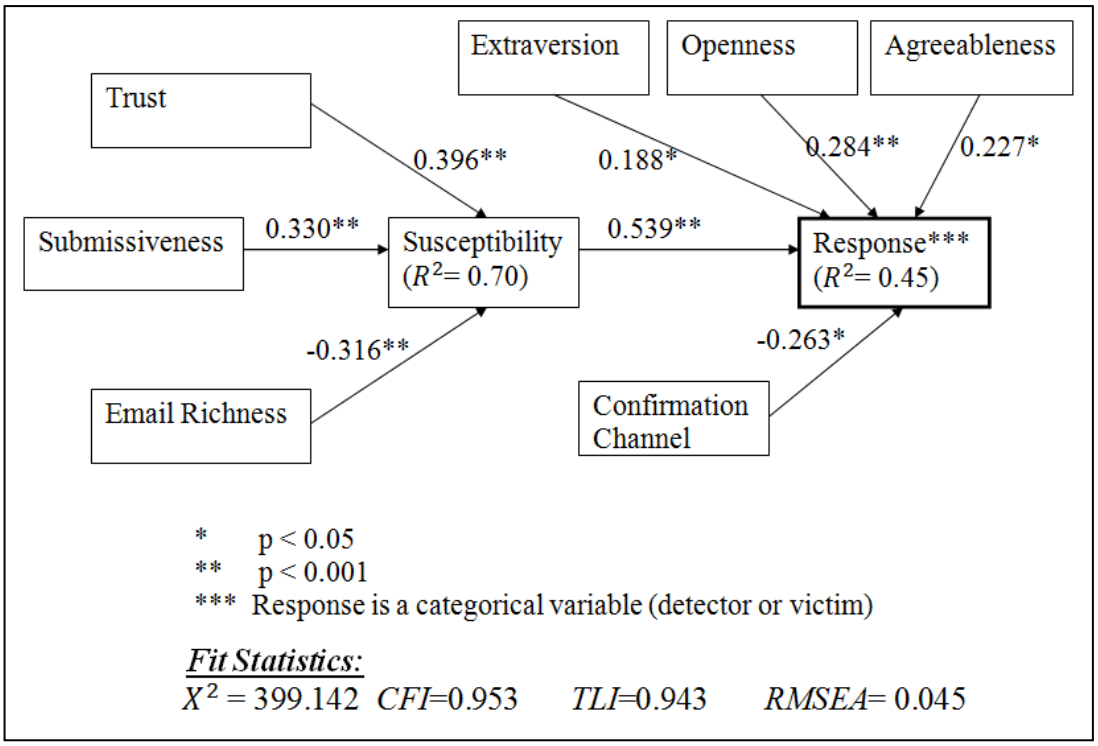

Figure 32: Structural model for Australian study

Table 64: R software results - Australia

Path		Path	Standard	
ID	DV	coefficient	error	P-value
Trust	Susceptibility	0.396	0.067	0.000
Submissiveness	Susceptibility	0.330	0.067	0.000
Email Richness	Susceptibility	-0.316	0.083	0.000
Susceptibility	Response	0.539	0.019	0.000
Openness	Response	0.284	0.030	0.000
Extraversion	Response	0.188	0.029	0.018
Agreeableness	Response	0.227	0.032	0.019
Channel	Response	-0.263	0.024	0.032

Table 65: R square values - Australia

	R square
Susceptibility	0.703
Response	0.450

5.6 Summary

This chapter has described how we analysed the data from both the Saudi Arabian and Australian studies. The analysis began with preparation of the data to be entered into the analysis software. The chapter has presented the descriptive outcomes of data and explained how data validity and reliability were tested. We also explain how we tested the hypotheses and the final model. Hypothesis testing was conducted using multiple regression and logistic regression. The final model was tested with R software with Lavaan packages.

The results from the Saudi Arabian study show that users' submissiveness increases their susceptibility to phishing emails. Users' high level of susceptibility and their open personality increase their tendency to respond to phishing emails. The results from the Australian study support this finding from the Saudi Arabian study. The results from the Australian study show that users' submissiveness, in addition to trust, increases users' susceptibility. Users' high level of susceptibility and their openness, as well as extraversion and agreeableness, increase their tendency to respond to phishing emails.

Chapter 6: Qualitative Analysis

This chapter presents the results of our analysis of the qualitative data obtained from interviews. The main purpose of this method was to generate deeper understanding of users' detection behaviour and of the differences between detectors and victims. Qualitative data is intended to answer questions 1, 2, and 3. The setting of the interviews was explained earlier (see Section **Error! Reference source not ound.**) and the research questions can be found in the Appendix B.

The chapter begins by explaining the measures of reliability and validity that were applied to these results. The process used to analyse the data is then described. Finally, the findings are presented and interpreted.

Invitations to participate in an interview were sent to those participants who were classified as detectors or victims (see Section 4.9.5) and had completed the second survey. Both detectors and victims responded to the invitation. A total of 17 participants agreed to be interviewed, nine of whom were classified as detectors and eight as victims (see Section 4.9.5).

6.1 Reliability and Validity

The reliability of our method was assessed using the Cohen's Kappa index of inter-rater reliability (Carletta, 1996), which is often used to measure agreement between coders in qualitative research. Seven of the interviews were analysed by two different coders. Both were provided with transcripts of the interviews and the interview codebook and they conducted their analyses separately. The initial coding was based on four *a priori* topic categories that were derived from the MDD model. The results show a satisfactory level of agreement since the K value is above 0.7 (see Table 66). The codebook itself is displayed in Table 67. Please note that the first raw in Table 66 shows the themes used to categorise codes which are described in Table 67.

Table 66: Inter-coder reliability

Unit	Activation	Hypothesis generation	Hypothesis evaluation	Global assessment
Participant 1 a	**1**	**1**	**1**	**1**
Participant 1 b	1	0	1	1
Participant 2 a	**1**	**1**	**1**	**1**
Participant 2 b	1	0	0	1
Participant 3 a	**1**	**1**	**1**	**1**
Participant 3 b	1	0	0	1
Participant 4 a	**1**	**0**	**1**	**1**
Participant 4 b	1	0	1	1
Participant 5 a	**1**	**0**	**1**	**1**
Participant 5 b	1	0	0	1
Participant 6 a	**0**	**0**	**0**	**1**
Participant 6 b	0	1	1	1
Participant 7 a	**0**	**0**	**0**	**1**
Participant 7 b	1	1	1	1

		b	
		Agree	Disagree
a	Agree	14	6
	Disagree	10	12

Pr (a):= [(Coder 1 agree & Coder 2 agree) + (Coder 1 disagree & Coder 2 disagree)/ all cases]
And that equals 0.92
Pr (e):= 0.5

$$\kappa = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)},$$ (Galton, 1892)

K= 0.85

The inter-coder reliability is satisfactory because k > 0.7

The validity of our findings was assessed by comparing them with findings from the survey (i.e. data triangulation) (Emory & Cooper, 1991; Sekaran, 2003).

6.2 Analytic Procedure

As explained in Chapter 3, most of the interviews were audio recorded and additional notes were taken by the interviewer to capture important information. Only one participant requested to not record the interview. Therefore, only notes were taken during that interview. Each recorded interview was transcribed in full, yielding 16 transcripts, each of three to four pages in length.

The qualitative data were analysed in four phases. The first three phases were data reduction, data display and conclusion drawing (Miles and Huberman(1994). The final phase, data interpretation, integrated the findings from the previous three phases (Silverman, 2006).

6.2.1 Data reduction

Data reduction involves selecting those segments of the raw data which should be the focus of attention, and transforming these into a manageable form (e.g. a theme) (see Table 67).

Table 67: Codebook for analysis of the interviews

Phase	Description
Activation	Refers to the phase in which a user **suspects** the existence of a phishing email. Suspicion begins by observing inconsistency between what users expect to see in real emails and what they actually observe in the phishing email.
Hypothesis generation	Refers to the phase in which a user **develops an explanation** for the inconsistency (*interpretation of the inconsistency*).
Hypothesis evaluation	Refers to the **processes** that a user chooses to test the explanation (*interpretation of the inconsistency*).

Global assessment	Refers to the **final decision** a user makes based on the combined results from hypothesis evaluation.

6.2.2 Data display

Data display refers to how the information is organised and presented for analysis. In the present study, the data were displayed in the form of a table in which the participants were divided into two groups (detectors and victims) and their responses were listed under each *a priori* topic category. Data that could not be classified under one of these categories were grouped in a separate category for further analysis (Braun & Clarke, 2006).

6.2.3 Conclusion drawing

This refers to the process of identifying regularities and patterns in the data and their related conditions and consequences (Glaser, 1978).

6.2.4 Data interpretation

The final phase in qualitative data analysis is interpretation, in which the results from the previous phases are integrated. In this phase, dominant and emergent themes are identified. The dominant themes from our analysis were detectors' behaviour and victims' behaviour, each of which contained several sub-themes. The emergent themes were: perceived account importance, communication between users, awareness of phishing email cues, and choosing whom to consult.

6.3 Results

The results obtained from the interview analysis are presented in this section.

6.3.1 Detectors' behaviour

Detectors identified the phishing email and chose not to comply with its request. The analysis revealed three main factors that differentiated detectors from

victims (see Table 68): perceived negative consequences; knowledge of phishing email cues; and high importance of the requested information.

Perceived negative consequences. Detectors ignored the phishing email because they believed that responding might be harmful to them.

Knowledge of phishing email cues. Knowledge of the existence of phishing emails by itself appears to not prevent users from responding to them. Unlike victims in the present study, detectors knew how to identify cues which led them to identify phishing emails, such as requests for passwords.

High importance of the requested information. Some detectors ignored the phishing email because they thought the requested information was too important to reveal. This was an important source of difference between detectors and victims. Table 68 illustrates detectors' responses to the question of why they did not perform the action requested in our phishing email.

Table 68: Detectors' responses

Code	Excerpt from transcript
Negative consequences	"I am afraid that the attacker will identify me as a vulnerable user and send me harmful emails"
Low security behaviour	"I did not respond because I know this kind of action is behaviour of phishing emails. That is why I did not respond"
Importance of the requested data	"I did not respond with my password because it is not a secure behaviour to send password via email. Most importantly, my password is very important to me because it is linked to my other accounts which are very important. If I lose my password, I will lose valuables in my other accounts"

As can be seen from these responses, detectors felt responsible for protecting their information and behaving securely. They did not shift the responsibility for protection onto others.

Detectors were asked to identify the source of their knowledge about phishing emails. They gave a variety of responses, including: 1) general publicity about the

negative consequences of losing private information, such as identity theft; 2) specific warnings about phishing emails associated with online gaming and how these can be identified; 3) personal experience in designing websites, which gave them insight into their weaknesses and how these weaknesses can be exploited by attackers.

6.3.2 Victims' behaviour

Most phishing email studies classify users into two main categories: victims and detectors. This classification is based on the final behaviour (i.e. respond or not). Our investigation, however, identified three types of victims: naïve victims, doubtful victims and risk-taker victims based on the investigation of users' detection behaviour (see Figure 33).

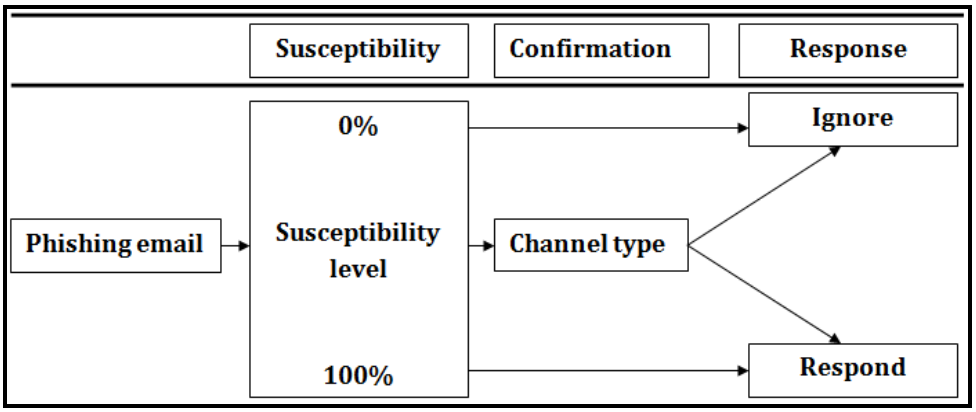

Figure 33: Users' behaviour when faced with phishing emails

6.3.2.1 Naïve victims

Naïve victims have little or no suspicion (i.e. they have high levels of susceptibility). Most did not generate or evaluate a deception hypothesis. Their explanation support the deception by believing that the phishing email is real. Their suspicion levels were very low, they believed the phishing email was real, and as a result they responded directly to it (see Table 69). Significantly, they had not even considered the possibility of a phishing email before they responded. They had no doubts about whether it was legitimate.

Table 69: Naïve victims

Code	Excerpt from transcript
No suspicion	"I thought it was some routine check and that something had happened. I did click on the link and reset my password. I did not think it would have any effect. I thought it was from the university, like some sort of support."
New situation	"The first unit that I took, which had a classroom blog; this made me think that the email came from the lecturer because a problem had occurred in the blog."
Trust	"I did not have any doubts because it came from the official university website." "No. Because it is from my university and my university is a trustworthy educational institution."

The quantitative data suggested that certain personality characteristics, such as trusting new people, low perceived email richness and high submissiveness increase users' susceptibility to phishing emails. These characteristics were found to be negatively associated with users' suspicion. Thus the quantitative data support the findings from the interviews (i.e. users with low suspicion respond to phishing emails directly).

6.3.2.2 Doubtful victims

Doubtful victims suspected the phishing email but failed to confirm their suspicion. Their weakness was that they lacked a strong confirmation channel (see Table 70).

Table 70: Doubtful victims

Code	Excerpt from transcript
Weak confirmation channel	"I asked some of my colleagues if they received the same email. Then, I realised that all of them had received the same email."
Verification with peers	"After I asked my university colleagues if they received the email, my doubt was gone when they confirmed that they also received the email."
Consult a victim	"In the beginning I had doubts, but in the end I felt safe because the email was from the university."

The quantitative data support these findings. The type of confirmation channel has a significant impact on users' accuracy in detecting phishing emails. Users who chose to authenticate the phishing email by consulting others were more likely to detect phishing emails than those users who depended on themselves for detection.

6.3.2.3 Risk-taker victims

Risk-taker victims chose to respond to the phishing email because they did not see any harm in adopting low-security behaviour. These victims did not lack knowledge about phishing emails or secure behaviour. Two main factors were associated with this risk-taking behaviour: the level of importance participants ascribed to the requested information, and the perceived negative consequences (see Table 71). In interview, these victims reported that they felt the requested information was not worth protecting and did not believe that behaving less securely would cause them any harm (such as loss of their blogs).

Table 71: Risk-taker victims

Code	Excerpt from transcript
Perception of low- risk consequences	"I trust that the university will understand my situation if my blog is damaged. The worst case scenario is I lose the content in the blog. In this case I can contact the lecturer and tell him about what happened." "I know that what I did is wrong; I should not send my password. However, I thought that the email came from the lecturer himself."
Protecting requested information is not important	"For me, the password's importance is related to its purpose. For example, passwords for my bank account and other important accounts are very important to me. On the other hand, passwords for forums and blogs are less important to me." "In the blog, the content is stored with me. I will not lose anything"

The quantitative data support these findings. There was a significant relationship between certain personality characteristics, such as extraversion and openness, and users' response to phishing emails. Users with these characteristics are more willing to accept and experience new ideas. For some participants in our study, phishing emails may be a new experience. Some acknowledged that sending passwords via email constitutes low-security behaviour but they did not worry about complying with the request. Their explanation was that they would not lose anything if someone obtained their passwords.

6.3.3 Emergent themes

The analysis identified several additional factors that directly influenced users' detection behaviour. These factors were: perceived account importance, communication between users, awareness of phishing email cues, and choosing whom to consult. Each is discussed below.

6.3.3.1 Perceived Account Importance

An important factor in some victims' decision to respond to the phishing email was the perceived importance of protecting their account. These victims responded because they did not think their account was important, so they were not concerned about losing it (see Table 72).

One participant, for instance, reported that he knew about phishing emails and the dangers associated with them. In fact, he had lost online accounts as a result of phishing emails in the past. He also described another incident in which he had received a phishing email that pretended to come from his bank. His response on that occasion (he called the bank directly and informed them about the incident) was very different from his behaviour in our study (he responded to the phishing email). The participant himself explained the difference between these behaviours as the result of perceived level of importance. If the email supposedly from his bank was a phishing email, he could lose money. On the other hand, he had no important information in his blog account and was not worried about losing it. Even if this happened, he could prove to the authorities (i.e. the lecturer) that he had completed the unit requirements and was eligible to receive the unit marks for the blog assignments.

Similarly, another victim in our study acknowledged that he did not think about the consequences of responding to the phishing email. He responded as soon as he opened the email. He admitted that he knew he should not send passwords via email but, when asked if he would send his blog password if the lecturer asked him to, he stated that he would do so. He explained this behaviour in relation to the nature and importance of the account. Bank accounts, for example, are very important and their passwords should be difficult. Bank passwords should contain letters, numbers and symbols. Other less important accounts, such as blogs and forums, do not need such complicated passwords. Thus he behaved less securely in protecting his blog password, as he considered it less important.

Table 72: Perceived account importance

Code	Excerpt from transcript
No losses	"I have a backup in my computer. So anything lost in the blog I can retrieve it from my computer. "The significant difference is the interest. The Bank and PayPal related to my money. I will lose my money and I can't retrieve it. In the blog, the content is stored with me, so I will not lose anything."
Different classification for different accounts	"The password importance is related to its purpose. For example, passwords for my bank account and other important accounts are very important to me. On the other hand, passwords for forums and blogs are less important to me."

6.3.3.2 Communication between users

The interviews revealed very low levels of communication (warnings) between users themselves, particularly by participants who were early detectors of the phishing email. When asked if they warned other users about their discovery of the phishing email, many said that they did not do so. Such detectors mainly focused on warning a relevant authority. Their reasoning was that the authority responsible for protection would take the necessary steps to warn other users (see Table 73).

In our study, we were only able to make a limited assessment of the impact of a warning from an authority. A relevant authority (the lecturer) could warn users after a certain time that a phishing email had been sent. It was anticipated that early warning from an authority would increase the detection rate and may reach users who had not yet opened the phishing email. Therefore, the warning was sent after allowing time for users to decide on their response (see Section 4.8).

As mentioned previously, detectors themselves displayed different forms of warning behaviour. Some warned the owner of the server while others did nothing after they had detected (and ignored) the phishing email.

Table 73: Users' responses to the phishing email

Code	Excerpt from transcript
Detectors	"If he (the owner of the server) sees the email from me he will say hang on I did not sent this email. Then he will know that his email has been compromised" "I did not want him (the lecturer) to tell me what to do. I forwarded it to him because he has to do what he should do"
Doubters	"I was not sure if it was a scam or not. But I am pretty sure that there is something fishy, dodgy. So, I consulted the lecturer to tell me what to do" "If the lecturer is aware of this he will advise us what to do next"
Victims	Respond by clicking or replying

The findings indicate that communication between participants was extremely low. Participants who detected the email as a phishing email did not take the initiative to warn their peers. Yet detection time is crucial. In the Australian study, for example, some participants detected the phishing email in its early stages (first three hours), which was the period during which nearly half of the victims responded to the phishing email.

6.3.3.3 Awareness of phishing email cues

Many studies propose that awareness of phishing emails can increase users' protection. Indeed, this is the main or only aim of many phishing email education programs. Our qualitative data, however, show that awareness alone did not prevent some participants from responding to the phishing email. The majority of identified victims had heard about phishing emails and some had fallen victim to them in the past. In this context, the main difference between victims and detectors is that detectors were able to identify certain cues as signs of phishing emails while victims were not (see

Table 74).

Table 74: Awareness of phishing emails

Participant	Excerpt from transcript
Detector (Participant 2)	"I got this information from the Internet. I play video online games and often people will send you emails like the email you sent asking for your details."
Detector (Participant 1)	"I am from 'a specific country' and we have strict security rules and we are very aware of phishing emails; most of them are usually from banks."
Victim (Participant 6)	"Yes, I heard about them (phishing emails). They send a program through email. When a user opens this email they can steal your information."
Victim (Participant 7)	"Yes, I know about it but I am not interested in it."

As Table 80 shows, detectors have specific knowledge about how phishing emails work and how to identify them. On the other hand, victims had heard about phishing emails but did not know how to identify them.

6.3.3.4 Choosing whom to consult

Some doubtful users consulted others to help them decide. One of our research objectives was to examine the impact of the richness of the confirmation channel on users' detection ability. The qualitative data suggested that the choice of person to consult was also important.

The qualitative data suggested that both richness of the confirmation channel and the type of person consulted affect users' detection behaviour. One participant, for example, consulted his friend, who was also a victim. The friend said that he had responded to the phishing email, which encouraged the participant to do so as well. In other words, despite the use of a rich medium (face to face) as the confirmation channel, this user became a victim.

Table 75: Choosing Whom to Consult

Participant	Excerpt from transcript
Detector (Participant 16)	"I did not respond to it. I asked a couple of my friends whether they received it as well. They said they were going to ask the lecturer. They asked the lecturer and he said do not respond to emails that ask about passwords."
Detector (Participant 4)	"Then, I sent an email asking the lecturer about that email. The admin can reset the password, so why would they ask about it?"
Victim (Participant 10)	"I did make sure by asking my colleagues if they had received this email."
Victim (Participant 6)	"I asked some of my colleagues if they received the same email. Then, I realised that all of them had received the same email."

Table 75 shows that the type of person consulted affects the likelihood of users becoming victims. Consulting the appropriate person increases users' chances of becoming detectors, while consulting an inappropriate person increase their chances of becoming victims.

6.4 Summary

This chapter has presented the findings from analysis of the qualitative data. Three main factors were shown to differentiate detectors from victims: perceived negative consequences; knowledge of phishing email cues; and high importance of the requested information.

Our findings extend previous work by identifying three categories of victims: (1) naive victims, who did not even suspect the phishing email and responded directly to it; (2) doubtful victims, who suspected the phishing email but failed to confirm their suspicion; and (3) risk-taker victims, who knew that their action (sending passwords via email) was a form of low-security behaviour but performed the action because they perceived it to be harmless. Detectors, by contrast,

demonstrated greater care and responsibility in relation to protecting their passwords and behaved more securely.

An unexpected finding was that the majority of detectors simply ignored the phishing emails but took no steps to warn others. Some, however, warned an authorised person who, they believed, had the responsibility to warn others. Such warnings need to be sent immediately following detection if the authorised person is to be able to take appropriate action. Only some detectors did this.

Chapter 7: Discussion

This chapter begins by summarising the findings of our research. Our results confirm that users' detection behaviour has three main phases and that certain users' characteristics affect these phases. This is followed by a discussion of the main differences between the two studies (Saudi Arabia and Australia). Next we discuss the implications of our findings in relation to strategies for improving users' protection against phishing emails. The chapter concludes with recommendations for each of the main stakeholders in the search for solutions to the problem of phishing emails: victims, IT professionals and organisations.

7.1 Summary of Findings

The aim of our research was to identify weaknesses in users' detection behaviour and the characteristics that affect that behaviour. Our results show that several characteristics impact on users' detection behaviour and differentiate between detectors and victims. Some characteristics increase users' vulnerability to phishing emails while others reduce their vulnerability. Figure 34 presents an answer to the first question in our research (Q1) and summarises the findings in relation to three phases: susceptibility, confirmation and response (see also Figure 9).

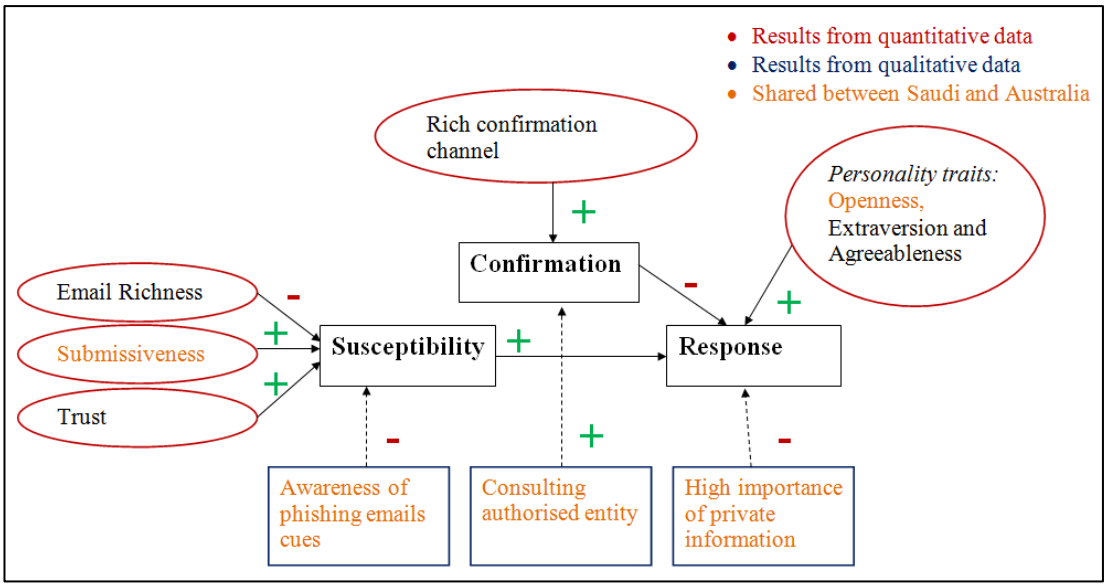

Figure 34: Impact of users' characteristics on phases in detection behaviour

In order to answer the second and third questions (Q2 and Q3), the following paragraphs present our findings. The process of detection begins with awareness of phishing email cues. Awareness is essential if users are to identify phishing emails and is a key consideration in reducing their susceptibility.

Susceptibility is affected by perceived email richness (a user characteristic), which increases the number of cues upon which users can draw to determine the legitimacy of an email and, hence, enhance their protection. In this context, it is important to note, email is considered a poor medium that presents insufficient cues for a reliable judgment.

Phishing email cues are one of the triggers for detection. Identification of these cues requires attention to certain features that ordinary users may neither notice nor understand. Perceived high email richness helps detectors to extract the relevant cues from phishing emails.

Users' susceptibility is increased by two characteristics—trust and submissiveness. Both of these characteristics can be exploited by the perpetrators of a phishing email attack. Phishing emails ask users to trust them by impersonating trustworthy entities. Users with high levels of trust and submissiveness are less likely to question the legitimacy of emails that pretend to come from a trustworthy entity.

Users who do not question the legitimacy of emails that purport to come from trustworthy entities need to be informed that if they do suspect an email, this does not mean they suspect the entity itself.

High submissiveness also increases users' susceptibility. Highly submissive users are more likely to obey orders, and this decreases their ability to question the instructions in a phishing email. Phishing emails always make a direct request for the recipient to comply with a specified action. Hence high submissiveness increases users' susceptibility to phishing emails.

The second phase in users' detection behaviour is confirmation. Our findings showed that the confirmation phase is affected by two main factors: the type of confirmation channel (quantitative data) and the type of person consulted (qualitative data). A rich confirmation channel helped users to identify phishing emails and reduced the likelihood that they would respond to phishing emails.

The qualitative data showed that the choice of person to consult also affected participants' ability to detect phishing emails. The choice of a person with the appropriate knowledge, such as a server administrator or IT expert, helps users to identify phishing emails. For example, server administrators are likely to know whether the email was initiated from the institution. An IT expert, on the other hand, knows how to distinguish phishing emails from legitimate ones. Our findings suggest that it is more beneficial to consult an authorised person within an organisation rather than an IT expert because the former can provide an unequivocal answer as well as warn other potential victims.

The third phase in users' detection behaviour is response. The survey identified three personality characteristics that increase users' response to phishing emails: openness, extraversion and agreeableness. The qualitative data provided additional insight by suggesting that the level of importance users assign to the requested information influences their response. Participants who perceived the requested information as relatively unimportant were more willing to take the risk of responding.

Clearly, defences against phishing emails need to address all potential weaknesses in users' detection behaviour. Concentrating on only one area of

weakness leaves other users, who have a different weakness, still vulnerable. As our qualitative data showed, there are at least three types of victims, each with its own areas of weakness.

Question four (Q4) is answered by comparing the findings between the two group of participants Saudi Arabian and Australian participants. Culture was also found to impact on users' ability to detect phishing emails. Both intracultural (within Australia) and cross cultural (Saudi Arabia and Australia) differences were observed. The Australian study included participants from different cultural backgrounds. Native Australian participants were found to be less vulnerable to phishing emails from Australian sources than their counterparts from other cultures. The likely explanation for this is that Australian nationals, whose first language is English and who are familiar with local organisational practices, are better able to detect linguistic and cultural cues of phishing emails.

Saudi Arabian participants were less vulnerable to phishing emails than Australian participants. The reasons for this are discussed below.

7.2 Comparative Analysis of the Saudi Arabian and Australian Studies

Both studies were similar in overall design. In the first stage, a survey was used to collect information about users' characteristics and levels of susceptibility. In this survey, users were not informed about the actual intention of the research (i.e. that it concerned phishing emails). In the second stage, users were sent phishing emails asking them to reveal their secret information (passwords). Their actions (i.e. respond or ignore) were recorded. In the third stage, users were sent a second survey that informed them of the real intention of the research and collected information about the confirmation behaviour they had employed when they received the phishing email. In the final phase, survey respondents who had been identified as detectors or victims were invited to participate in an interview. The key difference between these two studies is culture. The Saudi Arabian study was conducted in Saudi Arabia where Australian study was conducted in Australia (see Section 4.9).

There were two main differences in the results of these two studies: the response rate (see Section 7.2.1) and the number of users' characteristics that had an impact (see Section 7.2.2). The number of victims in the Saudi Arabian study was significantly lower than the number of victims in the Australian study. In addition, fewer users' characteristics were identified in the Saudi Arabian study than in the Australian study. The reasons for these differences are discussed below. Overall, however, the results from both studies support each other.

7.2.1 Number of victims

There were 14 victims (4%) of the total study population in Saudi Arabian study and 112 victims (26%) of the total study population in the Australian study. This was a significant difference. Two factors accounted for the difference: the perceived importance of email as a communication channel and differences in users' characteristics. The second cause is considered in Section 7.2.2.

The first factor can be explained in terms of social presence. Social presence measures the level of effectiveness of a medium by its ability to include interpersonal involvement required for a certain task (Miranda & Saunders, 2003). Contributing factors are as follows:

1. Unlike the Australian participants, the Saudi Arabian participants do not check their emails regularly. This was evidenced in the observed response time among victims in both studies.

2. In the experience of the student researcher, who is a Saudi Arabian national, email is not viewed as an important and reliable medium for communication by Saudi Arabian users. By contrast, Australian users regularly check their emails and use emails for work.

3. Some participants in the Saudi Arabian study had to be instructed to activate their university email account in order to communicate with the lecturer, which supports the suggestion that email does not have high importance as a communication channel in Saudi Arabia. In the Australian study, all participants already had an active email account and they used it to communicate with their lecturer.

4. In Saudi Arabia, the majority of online services, such as banking, do not use email as an official communication channel. Offers and notices from banks are mainly sent via short message system (SMS) to clients' mobiles. In Australia, most updates are sent via email unless an urgent response from clients is needed.

The number of Saudi Arabian victims is expected to increase in the future, as email becomes more widely accepted as an important medium for communication. Saudi Arabia is still a developing country in relation to the importance and spread of the e-services provided in both the private and public sectors. The Saudi Arabian government, however, is moving towards providing its own services online and encouraging organisations to do so (Yesser, 2013). As more citizens connect to the Internet, the chances of users receiving phishing emails increase. Since users are the weakest link in the protection chain, appropriate action is needed to educate them about the problem of phishing emails.

7.2.2 Differences in users' characteristics

Certain characteristics were similar in both studies. These included trust, submissiveness, perceived email experience and richness, and susceptibility to phishing emails. There were differences in Internet and email experience, preferred type of confirmation channel and Big Five personality dimensions.

Both Saudi Arabian and Australian participants agreed that they are more likely to trust others. Participants from both studies mainly agreed on submissiveness and on the final item (*they do not let others criticise them or put them down without defending themselves*). There were no significant differences in perceived email experience and richness. Participants in both studies had the same susceptibility to phishing emails. In both studies, participants were more susceptible to bank phishing emails and less susceptible to university or scam emails.

Saudi Arabian and Australian participants differed in relation to Internet usage and email usage. On average, Australian and Saudi Arabian participants had used the Internet for 10 years and 7 years, respectively. Australian participants spent, on

average, more time (5.4 hours) using the Internet than Saudi Arabian participants (3.2 hours). Australian and Saudi Arabian participants had been using the email service, on average, for 9 years and 6 years, respectively. On the other hand, there were no significant differences in average number of years using the university email service or in the number of emails received per day. This latter observation is accounted for by the fact that the most participants in both studies were undergraduate students in their second year of university.

Clearly, Australian participants had longer histories of Internet and email service usage than Saudi Arabian participants. Users with more experience are expected to be more likely to detect phishing emails. Yet our study found more victims in Australia than in Saudi Arabia. At the same time, our results show that native Australian users were significantly better able than non-Australian users to detect the phishing email used in the study. Why, then, were there more victims in the Australian study? The most likely explanation for this is that the phishing emails used in the Australian study were written in English and impersonated an Australian organisation. It can be concluded that native Australians are better at spotting problematic issues in language and local organisational policy than are those whose first language is not English or are less knowledgeable about Australian culture and organisational practice.

There were also differences between the studies in preferred confirmation channel. In the Saudi Arabian study, users preferred confirmation channels that involved asking others (endorsing behaviour). In the Australian study, users preferred to depend on themselves for confirmation (investigation behaviour). In the survey, Saudi Arabian participants scored highly on the item *asking others via telephone* and recorded low scores on the item *making a decision without consulting others*. In the Australian study, these scores were reversed.

These differences can be explained as the result of cultural differences. Saudi Arabian culture endorses collectivism while Australian culture endorses individualism (Hofstede, 2011). Individualism encourages people to depend on themselves rather than others. Therefore, Australian participants chose to depend on themselves to authenticate the legitimacy of the phishing emails while the Saudi Arabian participants chose to consult others for this purpose.

Our findings showed that the confirmation channel played an important role in influencing users' behaviour towards phishing emails. Specifically, choosing a rich confirmation channel decreased users' vulnerability. Saudi Arabian users were more likely to choose a rich confirmation channel (i.e. phone). Australian participants, who were more likely to depend on themselves for evaluation, were significantly more vulnerable.

The Big Five personality dimensions were ordered differently in the two studies. Saudi Arabian participants were more conscientious and less agreeable. Australian participants were more open and less emotionally stable. Average extraversion scores were the same in both studies. These differences suggest a further reason for the higher number of Australian victims. Previous research (Wright et al., 2009) suggest that users who were able to detect phishing emails scored highly on conscientiousness, as did our Saudi Arabian participants, while agreeableness has been shown to correlate with increased susceptibility to phishing emails (Srivastava, John, Gosling, & Potter, 2003). Our data also showed that openness increased users' response to phishing emails.

It is reasonable to conclude that culture does not directly affect users' ability to detect phishing emails. Rather, culture directly impacts on users' characteristics, and these characteristics have a direct impact on users' ability to detect phishing emails. For example, spotting spelling and other linguistic mistakes is a challenge for users who come from different cultures. Similarly, certain personality traits are more prevalent in some cultures than in others. Both studies showed that openness increases users' vulnerability to phishing emails, but Saudi Arabian users were more conscientious than open, while Australian participants were more open than conscientious.

7.3 Implications of our Findings for Protective Strategies

This section discusses the implications of our findings for the development of strategies to increase users' ability to detect phishing emails. In particular, we focus on the three phases in users' detection behaviour, each of which is associated with a particular weakness, as explained below.

7.3.1 Focus on email content

Victims of phishing emails focus more on the content in the body of the message. A recent study using eye-tracker technology found that even users with advanced technical knowledge spent more time on the email content than on meta-data when judging its authenticity (Pfeiffer et al., 2013). As explained in Chapter 2, phishing emails are designed to imitate legitimate email design in order to conceal deception and increase trust. Users who cannot spot the relevant cues are more vulnerable. According to Xun et al. (2008), the first weakness in victims' decision-making is the choice of unreliable cues to judge an email's legitimacy. Our findings show that this weakness is associated with three characteristics that increase users' susceptibility to phishing emails. These characteristics are trust, submissiveness and low perceived email richness.

Users with high trust and submissiveness are more vulnerable to phishing emails. It is difficult, if not impossible, to change an individual's personality characteristics but their effects can be reduced. Submissiveness, for example can be employed to increase users' protection against phishing emails. Highly submissive users are more likely to follow instructions. Hence, a direct instruction to protect their secret information that comes from an authoritative source can increase their protective behaviour (Wright et al., 2009). The effects of trust can be mitigated by informing such users that emails are not always trustworthy and their legitimacy should be checked.

Perceived email richness, on the other hand, has been shown to decrease users' vulnerability. Users who perceived email to be a rich medium were able to extract more cues than those who perceived email to be a poor medium. Users are more likely to detect deception conducted in a rich medium than in a poor medium (Daft & Lengel, 1986). Email richness can be achieved by improving users' knowledge and experience about emails and, especially, cues that aid detection of phishing emails.

Our qualitative data showed that knowledge of the existence of phishing emails does not improve users' defences, whereas knowledge of phishing email cues does do so. Both victims and detectors knew about phishing emails but victims did not know how to identify them. Security knowledge did not have any significant impact

on the likelihood of users being detectors (Wright et al., 2009). Many users believe that the perpetrators of phishing emails are not interested in targeting them and stealing their information (Alnajim, 2009; Herzberg, 2009). As a result, they take less care to authenticate the legitimacy of emails. Therefore, merely warning users about phishing emails is not sufficient.

7.3.2 Inability to follow up suspicion effectively

Observing inconsistent cues is an important aspect of the detection process in general (Buller & Burgoon, 1996). In relation to phishing emails, inconsistent observation occurs when users observe cues that differ from what they expected. When users observe inconsistent cues, they become suspicious about the email. Different types of confirmation channel are available for users to validate their suspicion.

The type of confirmation channel significantly affected participants' ability to detect phishing emails, and there were cultural differences in preferred confirmation channel. Saudi Arabian users chose a rich confirmation channel (consulting others by phone) while the Australian users chose to confirm their suspicion by themselves, without consulting others. This difference, we have proposed, reflects the fact that Saudi Arabian users come from a collectivist culture whereas Australian users came from an individualist culture. Choosing a rich confirmation channel increased users' chances of being detector.

We also found that the type of the person consulted has an important impact on the chances of users being victims. Those users who consulted other victims became victims themselves, since victims are unable to authenticate the legitimacy of an email. On the other hand, those users who consulted people in authority become detectors, since they received the correct information. For example, one participant who responded to the phishing email reported that he suspected that the email was illegitimate. He became a victim because he generated the hypothesis: "If other students received this email, then it is genuine". After contacting one of his friends, who confirmed having received the phishing email, he decided to respond simply because other students had received the same email. Because phishing emails target large numbers of users, this is clearly not a safe assumption. This is in sharp contrast

to the behaviour of detectors in our study. For example, one such participant forwarded the phishing email to the owner of the blog and asked if it was genuine. This allowed him to identify it as a phishing email.

7.3.3 Carelessness in dealing with emails

This weakness is affected by two main factors: perceived importance of the requested information and users' personality.

Perceived importance of the requested information prevented some detectors from responding to the phishing email. Victims, by contrast, attached low importance to their passwords and were not concerned about losing their information. The qualitative results showed that these victims responded to the phishing email because they did not consider that they would be harmed by this kind of low-security behaviour (i.e. sending their password via email). These victims knew about phishing emails and some had actually fallen victim to them in the past. This experience did not, however, prevent them from again engaging in low-security behaviour.

Certain personality dimensions also contributed to users' response. The survey results identified three such dimensions: openness, extraversion and agreeableness. Openness encourages users to be adventurous and try new experiences; hence they respond to phishing emails despite the potential risks involved. Extraversion encourages interaction with the phishing emails and the behaviour embedded in them. Agreeableness discourages suspicion and encourages a positive response to the requested action.

The combination of these personality traits increases users' risk-taking behaviour. This behaviour can be addressed by raising the stakes for a risky action (Burns et al., 2011).

7.4 Recommendations to reduce victimisation

From our findings, we have generated three sets of recommendations. These recommendations target victims, security tool designers and organisations, respectively.

7.4.1 Victims

We identified three types of victims: naïve, doubtful and risk-taker victims. Each has its own areas of vulnerability to phishing emails.

Naïve victims are vulnerable because they fail to observe and interpret the relevant cues (low suspicion). Their susceptibility is increased by their characteristics. The protection of such victims can be improved by enhancing their ability to suspect phishing emails. This can be accomplished by increasing their awareness of the design features of phishing emails.

Doubtful victims are vulnerable because they fail to choose an appropriate confirmation channel for their suspicion (medium suspicion). Their vulnerability can be ameliorated by forcing them to choose a rich confirmation channel. They also need to be informed that the best strategy is to communicate with an authorised entity.

Risk-taker victims' vulnerability is driven by their personality, which encourages them to engage in risky behaviour. They also attach a low level of importance to the requested information. These victims know that they are engaging in low-security behaviour (high suspicion), but continue to do so. They justify their behaviour through a belief that no harm will come to them as a result. In order to improve their defences, they need to change their perception of the level of risk involved in such behaviour.

7.4.2 Security tool designers

It has been reported that phishing websites have very short life spans, from hours to days (Moore & Clayton, 2007). This means that many security tools have limited ability to prevent phishing attacks on day Zero (Sheng et al., 2009). Designers need to investigate new ways of warning users in the early stages of a phishing email attack. We suggest that it would be beneficial to involve those users who are able to detect phishing emails in their early stages and who could report their discovery to the security tool designer.

7.4.3 Organisations

Organisations have some responsibility to protect their employees from phishing email attacks. In addition to implementing new security tools to prevent phishing emails from reaching users, organisations needs to find new ways of improving users' protection.

In one study (Kumaraguru et al., 2009), participants were divided into three groups: no training, one session of training and two sessions of training. On the final day of the experiment, there was a significant difference between the 'no training' group and the trained groups. Untrained participants, however, were able to identify phishing emails on days 2 and 7. This was because trained participants had discussed the training session with their fellow employees. Overall, 87% learned of the training from the original email, 5% from a forwarded copy of the original email, and 5% learned about it directly from their peers. Some 13% of participants discussed security tips provided by the security training with their peers. This suggests that information sharing can improve users' protection against phishing, and organisations can facilitate this type of behaviour.

Organisations should develop communication channels for their employees and encourage them to use these channels to warn about phishing attacks. There should be a website, email address or designated person with whom detectors can communicate to report new phishing attacks. In our experiment, only one person informed the university security department. This person was in fact a member of that department. Security departments should make themselves known to employees and share information. Our findings highlighted the importance of a reliable consultation source. To be effective, this source should be easily accessible to users.

Some of our study participants explained why they had not informed or consulted with their security department. They gave three main reasons: 1) they did not want to bother the department about an incident which the participant perceived to be of low importance to that department; 2) the department was not clearly identified (for instance, on the university's home page); 3) one participant thought that the department would not take the issue seriously and, if it did, the response would be too late (one or two days after the incident).

Organisations would benefit by encouraging detectors to report their discovery, thus enabling the organisation to warn others. Users who detect phishing emails should have a clear pathway for reporting their discovery to the relevant authority, which should be responsible for issuing a warning to other users. The response time could be significantly reduced in this way, since some users detect phishing emails at an early stage. More importantly, the warning should come from an appropriate authority rather than from colleagues. In a previous study, some detectors warned their colleagues about a phishing email but this did not prevent the colleagues from falling victim to it (Coronges et al., 2012). Wright et al. (2009), by contrast, found that warnings from an authorised person for users not to reveal their private information were effective in preventing some users from revealing their private information when they were exposed to the phishing email. The difference between these two studies is the source of the warning: in Wright et al.'s experiment, the person who issued the warning had authority over users, whereas in Coronges et al.'s experiment the warning came from colleagues who had no authority over them. This may help to explain the behaviour of risk-taker victims, who respond to phishing emails even when they are highly suspicious about them.

7.5 Summary

Users' detection behaviour comprises three phases. In each phase, certain characteristics impact on that behaviour and differentiate victims from detectors. Awareness of these relationships can help organisations to improve their protective strategies. The findings from two separate studies (Saudi Arabia and Australia) supported these findings. It can be concluded that the research model developed in this study can explain users' detection behaviour. Our findings have added to knowledge about users' weaknesses in detecting phishing emails and suggest ways of addressing these weaknesses through strategies directed at users, security tool developers and organisations.

Chapter 8: Conclusion

Chapter 1 of this thesis explained the research problem under investigation. Chapter 2 presented a critical review of literature and identified important gaps in knowledge about the topic. The causal model that was developed to guide the investigation was described in Chapter 4. The research design and methods used to test the model were explained in Chapter 5. Findings from the analysis of quantitative and qualitative data were presented in Chapters 5 and 6, respectively. The results were discussed in Chapter 7 and their implications for strategies to address the problem of phishing emails were considered. This chapter summarises the main academic and practical contributions of the thesis, discusses the limitations of the study, and presents guidelines for future work.

Our main findings can be summarised as follows;

- Users' detection behaviour has three main phases: susceptibility, confirmation and response.
- Users' characteristics have a significant impact on their detection behaviour in each phase.
- Culture impacts on users' ability to detect phishing emails.
- There is not a single type of victim and, therefore, no single solution to the problem of phishing emails. Protective strategies need to target specific vulnerabilities and weaknesses.

8.1 Academic Contributions

The main academic contributions of our research can be summarised as follows.

1. We have developed a model to examine the entire process of users' detection behaviour and identify weaknesses in their behaviour.

2. We have used quantitative data to identify the impact of users' characteristics on detection behaviour, in particular:

- the impact of trust, submissiveness and email richness on users' susceptibility;
- the impact of the type of confirmation channel on users' response; and
- the impact of personality traits on users' response.

3. We have used a qualitative method to identify additional factors that affect different phases in the model.

4. We have identified three categories of victims.

5. We have demonstrated the impact of culture on users' ability to detect phishing emails.

8.2 Contributions to Practice

The main contributions of our research to the development of practical strategies to address the problem of phishing emails can be summarised in relation to the three phases in detection behaviour and their vulnerabilities. These phases are: susceptibility, confirmation and response.

Susceptibility. Various studies have reported that educating users about phishing email cues can improve their detection ability. The ability to spot such cues alerts users to potential danger and prevents them from responding (Fette et al., 2007). Our data supported this finding and identified three characteristics that should be targeted in order to decrease users' susceptibility (see Section 7.3). These characteristics are trust, submissiveness and email richness. Trust can be addressed by educating users that phishing emails can impersonate any organisation and target any individual. Submissiveness has been found to increase users' susceptibility to phishing emails. At the same time, research has shown that the number of responders to phishing emails can be reduced by a direct instruction from an authorised person not to disclose private information (Wright et al., 2009). Thus the negative effects of

submissiveness could be addressed by issuing such authoritative directions and warning users about deceptive behaviour (i.e. priming). Email richness can be addressed by educating users about the various kinds of cues that help to identify phishing emails.

Confirmation. Our findings also showed that the choice of a rich confirmation channel and consultation with authorised personnel increased users' protection against phishing emails (see Section 7.3). While some users chose not to respond to phishing emails because they were suspicious of them, others harboured some suspicions but responded anyway. We found that users who chose a poor confirmation channel or consulted inappropriate sources (such as an inexperienced colleague) become victims. We also found that those who depended on themselves were more vulnerable. These findings strongly suggest that users should be encouraged to choose a rich confirmation channel and only consult with authorised personnel when they suspect a phishing email. Organisations have an important role to play here by providing their employees with clear communication channels and identified staff for contact in the case of a suspected phishing email.

Response. We found that some users who respond to phishing emails do so because of certain personality traits (see Section 7.3) that encourage them to take risks. Some victims responded to phishing emails because they did not see any need to behave more securely or to protect their private information. They also did not believe that any serious negative consequences would follow from their action. If such users are to be encouraged to behave more securely, they need to perceive the negative consequences of non-secure behaviour. Organisations can help in this regard by applying penalties for non-secure behaviour, such as revealing private information to others.

In summary, users' protection against phishing emails can be improved by:

1. Increasing users' awareness of phishing email cues.
2. Informing users that the organisation is a potential target for phishing email attacks.

3. Informing users about a deceptive behaviour such as requests for passwords.

4. Encouraging users to choose a rich confirmation channel to evaluate suspected phishing emails.

5. Encouraging users to consult with an authorised person about a suspected phishing email.

6. Encouraging users not to depend on themselves to evaluate a suspected phishing email.

7. Encouraging users to reduce their risk-taking behaviour when they suspect a phishing email.

8.3 Types of Victims

Our data showed that there is not a single type of victim. We identified three categories: naïve victims, doubtful victims and risk-taking victims. Each type has its own areas of weakness and, therefore, needs to be treated differently (see Section 7.3).

Naïve victims have low or no suspicion in relation to phishing emails. These victims' vulnerability occurs when they open the email and choose to respond directly. This area of vulnerability can be addressed by raising awareness of phishing emails through the development of appropriate educational programs and security tools that help users to identify phishing emails. Naïve victims fall prey to phishing emails because they have a high level of susceptibility in the first phase.

Doubtful victims have sufficient awareness to suspect phishing emails but fail to confirm their suspicions. In other words, they fail in the second phase of detection behaviour—confirmation. They do not use a robust confirmation channel. Rather, they are vulnerable because they test their suspicion through a poor confirmation channel. Their level of protection would be increased by providing them with information about suitable, rich confirmation channels that produce an immediate response and have their trust.

Risk-taking victims know that they are behaving less securely by responding to suspected phishing emails, but they assume that their behaviour will not have harmful consequences. Their personality encourages them to engage in dangerous behaviour, which increases their chance of falling victim to phishing emails. These victims ignore warnings about potential risks involved in responding to phishing emails. Organisations can address this behaviour by imposing a penalty for low security behaviour. Risk-taking victims are likely to choose a certain loss (not responding to suspected phishing email) over a higher potential loss (the penalty for responding). In addition, these victims do not attach high importance to protecting their private information. This perception can also be addressed by organisations. Organisations can increase the value of protecting private information by linking it to valued resources. For example, some banks do not reimburse funds that have been lost to a phishing attack if the user is responsible for disclosing their account information.

8.4 Limitations of the Study

In real life, users are exposed to more phishing emails than we tested. The research emails, however, imitated the behaviour of real phishing emails and their design incorporated features commonly used in most phishing emails (see Section 4.6). The study did not include all such design features, and the perpetrators of phishing email attacks will undoubtedly come up with new features. Nevertheless, the main design features used in our research will continue to be used.

The second limitation of our study is the age of participants (18 years and older). In real life, phishing emails can reach any user with an email address. Younger users are likely to be more vulnerable to phishing emails. A previous study, for instance, found users under 25 years of age are more susceptible to phishing emails than older users (Sheng et al., 2007). For ethical reasons, our study was limited to participants aged 18 years and above.

A third limitation is that those participants whom we identify as ‘victims’ did not actually provide their secret information to a phishing website. The study was not designed to capture such information. Rather, we identified participants who clicked

on the phishing email link as victims because other research has shown that most users who click on a link will continue to follow the instructions. In addition to the fact that these participants clicked on the link indicates that they had been deceived and, hence, warrant identification as victims.

Another important limitation is the fact that all participants in both studies were university students. The effect of this limitation was somewhat mitigated by the fact that they came from different countries and cultural backgrounds.

8.5 Recommendations for Future Research

Users are the last line of defence against phishing emails (see Section 2.6). Their defences should be constantly improved. While our research identified some weaknesses in users' detection behaviour and established the impact of some characteristics on these weaknesses, further research is needed to extend these findings and explore users' vulnerability in greater depth.

An important area for future experimental work is the impact of priming on users' ability to detection ability. Better understanding the impact of priming on users' ability to detect deception in phishing emails would enhance our knowledge of users' vulnerabilities.

Based on our findings, we recommend the development of a new warning system that could reduce the number of victims. We identified some users who were able to detect phishing emails at an early stage. It would be interesting to investigate the effect of implementing a system in which these early detectors were encouraged to warn authorities who, in turn, warned other users in an organisation.

We recommend that organisations develop rich confirmation channels that are cost-effective. The effects of instructing users to consult an authorised person using such rich channels could usefully be examined in relation to users' behaviour with suspected phishing emails.

We have also suggested that the imposition of penalties for poor security behaviour should reduce the number of users who respond to phishing emails. Empirical evidence is needed to verify this expectation.

The qualitative data in our research has found interesting findings. These findings can help is explaining the main differences between detectors and victims. A quantitative data can serve to find the significance of this impact statistically.

Finally, our identification of three types of email victims and their respective weaknesses provides the foundation for future work. It would be interesting, for instance, to examine whether some categories of victims are more or less likely to comply with recommendations to address their weaknesses.

Bibliography

Aburrous, M., Hossain, M., Dahal, K., Bradford, U., & Thabatah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Intelligent Techniques and Attack Strategies. *Journal of Cognitive Computation, 2*(3), 242-253. doi: 10.1007/s12559-010-9042-7

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *Security & Privacy, IEEE, 3*(1), 26-33.

Adams, J. E. (2012). *Mutual authentication and phishing–a clear case of user confusion.* (Master's degree MSc in Advanced Security and Digital Forensics), Edinburgh Napier University, Edinburgh, United Kingdom. Retrieved from http://www.jane-adams.com/wp-content/uploads/2012/09/janeadamsdissertation.pdf

Adelsbach, A., Gajek, S., & Schwenk, J. (2005). Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures. In R. Deng, F. Bao, H. Pang & J. Zhou (Eds.), *Information Security Practice and Experience* (Vol. 3439, pp. 204-216): Springer Berlin Heidelberg.

Allan, S., & Gilbert, P. (1997). Submissive behaviour and psychopathology. *British Journal of Clinical Psychology, 36*(4), 467-488.

Alnajim, A. M. (2009). *Fighting internet fraud: anti-phishing effectiveness for phishing websites detection.* (PhD), Durham University.

Anderson, D. E., DePaulo, B. M., Ansfield, M. E., Tickle, J. J., & Green, E. (1999). Beliefs About Cues to Deception: Mindless Stereotypes or Untapped Wisdom? *Journal of Nonverbal Behavior, 23*(1), 67-89. doi: 10.1023/a:1021387326192

Anti-Phishing Working Group. (2009). Phishing Attack Trends Report - Q4 2009. http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

Anti-Phishing Working Group. (2013). Phishing Activity Trends Report, 1st Quarter 2013. 11. http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf

Baron-Epel, O., Kaplan, G., Weinstein, R., & Green, M. S. (2010). Extreme and acquiescence bias in a bi-ethnic population. *The European Journal of Public Health, 20*(5), 543-548.

Baumgartner, H., & Homburg, C. (1996). Applications of structural equation modeling in marketing and consumer research: A review. *International Journal of Research in Marketing, 13*(2), 139-161. doi: http://dx.doi.org/10.1016/0167-8116(95)00038-0

Bekkering, E., Hutchison, D., & Werner, L. (2009). *A Follow-up Study of Detecting Phishing Emails.* Paper presented at the Proceedings of the Conference on Information Systems Applied Research 2009, Washington DC.

Bergholz, A., De Beer, J., Glahn, S., Moens, M.-F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of Computer Security, 18*(1), 7-35. doi: 10.3233/JCS-2010-0371

Bergholz, A., Paass, G., Reichartz, F., Strobel, S., Moens, M. F., & Witten, B. (2008). *Detecting known and new salting tricks in unwanted emails.* Paper presented at the CEAS 2008: Proceedings of the Fifth Conference on Email and Anti-Spam.

Bhattacherjee, A., & Sanford, C. C. (2006). Influence Processes for Information Technology Acceptance: An Elaboration Liklihood Model. *Mis Quarterly, 30*(4), 805-825.

Bond, C. F., & Atoum, A. O. (2000). International deception. *Personality and Social Psychology Bulletin, 26*(3), 385.

Bond, C. F., Omar, A., Mahmoud, A., & Bonser, R. N. (1990). Lie detection across cultures. *Journal of Nonverbal Behavior, 14*(3), 189-204.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi: 10.1191/1478088706qp063oa

Brislin, R. W. (1983). Cross-cultural research in psychology. *Annual review of psychology, 34*(1), 363-400.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory, 6*(3), 203-242.

Burns, M. B., Durcikova, A., & Jenkins, J. L. (2011). *Understanding Persistence of Risky IS Behavior with Respect to Phishing: A Multi-stage Approach.* Paper presented at the The 2011 Dewald Roode Workshop on Information Systems Security Research.

Carletta, J. (1996). Assessing agreement on classification tasks: the kappa statistic. *Comput. Linguist., 22*(2), 249-254.

Carlson, J. R., George, J. F., Burgoon, J. K., Adkins, M., & White, C. H. (2004). Deception in Computer-Mediated Communication. *Group Decision and Negotiation, 13*(1), 5-28. doi: 10.1023/B:GRUP.0000011942.31158.d8

Carlson, J. R., & Zmud, R. W. (1999). Channel expansion theory and the experiential nature of media richness perceptions. *Academy of Management Journal, 42*(2), 153-170.

Cavana, R. Y., Sekaran, U., & Delahaye, B. L. (2001). *Applied business research: qualitative and quantitative methods*. Milton, Qld: John Wiley & Sons Australia.

Chandrasekaran, M., Karayanan, K., & Upadhyaya, S. (2006). *Towards phishing e-mail detection based on their structural properties.* Paper presented at the New York State Cyber Security Confrance.

Chomsiri, T. (2007, May). *HTTPS Hacking Protection.* Paper presented at the Advanced Information Networking and Applications Workshops, 2007, AINAW '07. 21st International Conference on.

Cohen, J. (1960). A coefficient of agreement for nominal scales. *Educational and psychological measurement, 20*(1), 37-46.

Comrey, A. L., & Lee, H. B. (2013). *A First Course in Factor Analysis* Retrieved from http://QUT.eblib.com.au/patron/FullRecord.aspx?p=1562106

Cook, D., Gurbani, V., & Daniluk, M. (2009). Phishwish: A Stateless Phishing Filter Using Minimal Rules *Financial Cryptography and Data Security* (Vol. 5143, pp. 182-186): Springer Berlin / Heidelberg.

Cormac, H. (2009). *So long, and no thanks for the externalities: the rational rejection of security advice by users*. Paper presented at the Proceedings of the 2009 workshop on New security paradigms workshop, Oxford, United Kingdom.

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012). *The Influences of Social Networks on Phishing Vulnerability.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on, Maui, HI , USA.

Costa Jr, P., Terracciano, A., & McCrae, R. R. (2001). Gender differences in personality traits across cultures: Robust and surprising findings. *Journal of personality and social psychology, 81*(2), 322-331. doi: 10.1037/0022-3514.81.2.322

Costa, P. T., & McCrae, R. R. (1992). Four ways five factors are basic. *Personality and Individual differences, 13*(6), 653-665.

Creswell, J. W., & Plano Clark, V. L. (2007). *Designing and conducting mixed methods research*. Thousand Oaks, Calif. :: SAGE Publications.

Cyveillance. (2010). The Cost of Phishing: Understanding the True Cost Dynamics Behind Phishing Attacks. 8. https://www.cyveillance.com/web/docs/WP_CostofPhishing.pdf

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management science, 32*(5), 554-571.

Darlington, Y., & Scott, D. (2002). *Qualitative research in practice: stories from the field*. St Leonards, N.S.W: Allen & Unwin.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior, 26*(6), 1739-1747.

De Vaus, D. A. (2002). *Analyzing social science data*. London: SAGE.

Dhamija, R., & Tygar, J. D. (2005). Phish and HIPs: Human interactive proofs to detect phishing attacks. In H. Baird & D. Lopresti (Eds.), *Human Interactive Proofs* (Vol. 3517, pp. 127-141): Springer Berlin Heidelberg.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works.* Paper presented at the CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems, New York, NY, USA.

Dillard, J. P. (1994). Rethinkin the Study of Fear Appeals: An Emotional Perspective. *Communication Theory*, *4*(4), 295-323. doi: 10.1111/j.1468-2885.1994.tb00094.x

Dillard, J. P., & Pfau, M. (2002). *The persuasion handbook: Developments in theory and practice*: Sage Publications, Inc.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). *Decision strategies and susceptibility to phishing.* Paper presented at the SOUPS '06: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). *Behavioral response to phishing risk*. Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, Pittsburgh, Pennsylvania.

Egelman, S., Cranor, L. F., & Hong, J. (2008). *You've been warned: an empirical study of the effectiveness of web browser phishing warnings*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy.

Emm, D. (2006). Phishing update, and how to avoid getting hooked. *Network Security*, *2006*(8), 13-15. doi: http://dx.doi.org/10.1016/S1353-4858(06)70432-9

Emory, C. W., & Cooper, D. R. (1991). Business Research Methods . Boston: Richard D. Irwin. *Inc.*

Fette, I., Sadeh, N., & Tomasic, A. (2007). *Learning to detect phishing emails*. Paper presented at the Proceedings of the 16th international conference on World Wide Web, Banff, Alberta, Canada.

Field, A. (2009). *Discovering statistics using SPSS*: Sage Publications Limited.

Fink, A. (2009). *How to conduct surveys : a step-by-step guide* (4th ed.). Los Angeles :: SAGE.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *Technology and Society Magazine, IEEE*, *26*(1), 46-58.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Gable, G. (1994). Integrating case study and survey research methods: an example in information systems. *European Journal of Information Systems, 3*(2), 112-126.

Galton, F. (1892). *Finger Prints*. Macmillan, London.

Garfinkel, S. L., Margrave, D., Schiller, J. I., Nordlander, E., & Miller, R. C. (2005). *How to make secure email easier to use*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Portland, Oregon, USA.

Gass, R. H., & Seiter, J. S. (2007). *Persuasion, social influence, and compliance gaining (3rd)*: Boston: Pearson.

George, J. F., & Carlson, J. R. (1999). *Electronic lies: Lying to others and detecting lies using electronic media.* Paper presented at the AMCIS 1999 Proceedings.

Get Cyber Safe. (2013). Phishing: How many take the bait? Retrieved 5/9/2013, from http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

Glaser, B. G. (1978). *Theoretical sensitivity: advances in the methodology of grounded theory*. Mill Valley, California: Sociology Press.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the Big-Five personality domains. *Journal of Research in personality, 37*(6), 504-528.

GoslingLab. (2012). SCALES WE'VE DEVELOPED. Retrieved 15/3/2012, from http://homepage.psy.utexas.edu/homepage/faculty/gosling/scales_we.htm#Ten%20Item%20Personality%20Measure%20%28TIPI%29

Grazioli, S. (2004). Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. *Group Decision and Negotiation, 13*(2), 149-172. doi: 10.1023/B:GRUP.0000021839.04093.5d

Grazioli, S., & Wang, A. (2001). *Looking Without Seeing: Understanding Unsophisticated Consumers' Success and Failure to Detect Internet Deception.* Paper presented at the International Conference on Information Systems (ICIS), New Orleans, Louisiana, USA.

Gupta, M. (2007). Pharming Attack Designs *Encyclopedia of Information Ethics and Security* (pp. 520-526): IGI Global.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate data analysis* (Vol. 7): Prentice Hall Upper Saddle River, NJ.

Herley, C., & Florencio, D. (2008). *A profitless endeavor: phishing as tragedy of the commons*. Paper presented at the Proceedings of the 2008 workshop on New security paradigms, Lake Tahoe, California, USA.

Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *Computers & Security, 28*(1-2), 63-71.

Herzberg, A., & Gbara, A. (2004). Protecting (even) Naive Web Users, or: Preventing Spoofing and Establishing Credentials of Websites. *submitted to ACM CCS*.

Higgins, E. T. (1996). Knowledge activation: Accessibility, applicability, and salience. In E. T. H. A. W. Kruglanski (Ed.), *Social psychology: Handbook of basic principles* (pp. 133-168). New York, NY, US: Guilford Press.

Higgins, E. T., & Kruglanski, A. W. (1996). *Social psychology : handbook of basic principles*. New York :: Guilford Press.

Hofstede, G. (1993). Cultural constraints in management theories. *The Executive, 7*(1), 81-94.

Hofstede, G. (2001). *Culture's Consequences: International Differences in Work-Related Values* (2 ed.). Beverly Hills, CA. : Sage.

Hofstede, G. (2011). Countries - Geert Hofstede. Retrieved 25/10/2011, from http://geert-hofstede.com/countries.html

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping Up With The Joneses: Assessing Phishing Susceptibility in an Email Task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 57*(1), 1012-1016. doi: 10.1177/1541931213571226

Hutcheson, G. D. (1999). *The Multivariate Social Scientist. The Multivariate Social Scientist. SAGE Publications, Ltd*: SAGE Publications, Ltd.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Commun. ACM, 50*(10), 94-100. doi: http://doi.acm.org/10.1145/1290958.1290968

Jakobsson, M. (2007). *The Human Factor in Phishing*. Paper presented at the Privacy & Security of Consumer Information, Indiana University, Bloomington, USA.

Jakobsson, M., & Ratkiewicz, J. (2006). *Designing ethical phishing experiments: a study of (ROT13) rOnl query features*. Paper presented at the Proceedings of the 15th international conference on World Wide Web, Edinburgh, Scotland.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007). What instills trust? A qualitative study of phishing. *Financial Cryptography and Data Security, 4886*, 356-361.

James, L. (2006). Phishing exposed. Tech target article sponsored by: Sunbelt software. *available at: searchexchange.com*.

Jensen, A. R. (1998). *The g factor: The science of mental ability*: Praeger Westport, CT.

Johnson, P. E., & Grazioli, K. S. (1993). Fraud detection: Intentionality and deception in cognition. *Accounting, Organizations and Society, 18*(5), 467-488.

Johnson, P. E., Grazioli, S., Jamal, K., & Glen Berryman, R. (2001). Detecting deception: adversarial problem solving in a low base-rate world. *Cognitive Science, 25*(3), 355-392.

Johnson, P. E., Grazioli, S., Jamal, K., & Zualkernan, I. A. (1992). Success and failure in expert reasoning. *Organizational Behavior and Human Decision Processes, 53*(2), 173-203.

Juels, A., Jakobsson, M., & Stamm, S. (2007). *Active cookies for browser authentication.* Paper presented at the Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS '07).

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). *Assessing end-user awareness of social engineering and phishing.* Paper presented at the Proceedings of the 7th Australian Information Warfare and Security Conference.

Karlof, C., Shankar, U., Tygar, D., & Wagner, D. (2007a). Locked cookies: Web authentication security against phishing, pharming, and active attacks. In T. R. UCUCB/EECS-2007-25UCB/EECS-2007-25 (Ed.): Electrical Engineering and Computer Sciences University of California at Berkeley.

Karlof, C., Shankar, U., Tygar, J. D., & Wagner, D. (2007b). *Dynamic pharming attacks and locked same-origin policies for web browsers.* Paper presented at the CCS '07: Proceedings of the 14th ACM conference on Computer and communications security, New York, NY, USA.

Kim, Y.-G., Cho, S., Lee, J.-S., Lee, M.-S., Kim, I. H., & Kim, S. H. (2008). Method for Evaluating the Security Risk of a Website Against Phishing Attacks. *Intelligence and Security Informatics, 5075*, 21-31. doi: 10.1007/978-3-540-69304-8_3

Kleinginna, P. R., & Kleinginna, A. M. (1981). A categorized list of motivation definitions, with a suggestion for a consensual definition. *Motivation and emotion, 5*(3), 263-291.

Knight, W. (2004). Goin' phishing? *Infosecurity Today, 1*(4), 36-38. doi: 10.1016/s1742-6847(04)00089-8

Knight, W. (2005). Caught in the net [Internet and e-mail security issues]. *IEE Review, 51*(7), 26-30. doi: 10.1049/ir:20050702

Kumaraguru, P. (2007). PhishGuru: A System for Educating Users about Semantic Attacks *School of Computer Science* (Vol. Thesis Proposal). Pennsylvania, USA: Carnegie Mellon University.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). *School of phish: a real-world evaluation of anti-phishing*

training. Paper presented at the Proceedings of the 5th Symposium on Usable Privacy and Security, Mountain View, California.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). *Getting users to pay attention to anti-phishing education: evaluation of retention and transfer*. Paper presented at the Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, Pittsburgh, Pennsylvania.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008, 15-16 Oct. 2008). *Lessons from a real world evaluation of anti-phishing training.* Paper presented at the eCrime Researchers Summit, 2008.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*(2), 1-31.

Kuo, C. (2008). *Reduction of end user errors in the design of scalable, secure communication.* (Doctor of Philosophy), Carnegie Mellon University Pittsburgh, Pittsburgh.

Lee, J. K., & Rao, H. R. (2007). Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment. *Decision Support Systems, 43*(4), 1431-1449.

Li, T. Y., & Wu, Y. (2003). Trust on Web browser: Attack vs. defense. In J. Zhou, M. Yung & Y. Han (Eds.), *Applied Cryptography and Network Security* (Vol. 2846, pp. 241--253): Springer Berlin Heidelberg.

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology, 22 140*, 55.

Lin, K., Yuan, L., & Qu, G. (2007). *SecureGo: A Hardware-Software Co-Protection against Identity Theft in Online Transaction.* Paper presented at the Bio-inspired, Learning, and Intelligent Systems for Security, 2007. BLISS 2007. ECSIS Symposium on, Edinburgh, UK.

Maldonado, S., & L'Huillier, G. (2013). SVM-Based Feature Selection and Classification for Email Filtering. In P. Latorre Carmona, J. S. Sánchez & A. L. N. Fred (Eds.), *Pattern Recognition - Applications and Methods* (Vol. 204, pp. 135-148): Springer Berlin Heidelberg.

Mannan, M., & Oorschot, P. C. v. (2008). *Security and usability: the gap in real-world online banking*. Paper presented at the Proceedings of the 2007 Workshop on New Security Paradigms, New Hampshire.

Maslow, A. H. (1943). A theory of human motivation. *Psychological review, 50*(4), 370.

Maslow, A. H. (1954). *Motivation and personality*: NewYork:Harper.

Maslow, A. H. (1971). *The farther reaches of human nature*: New York: Viking.

McCornack, S. A., & Levine, T. R. (1990). When lovers become leery: The relationship between suspicion and accuracy in detecting deception. *Communication Monographs, 57*(3), 219-230.

McKnight, H., Kacmar, C., & Choudhury, V. (2003). *Whoops... did I use the wrong concept to predict e-commerce trust? modeling the risk-related effects of trust versus distrust concepts.* Paper presented at the System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on Waikoloa, Hawaii, USA.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: an expanded sourcebook.* Thousand Oaks: Sage Publications.

Miller, G. R., & Stiff, J. B. (1993). *Deceptive communication*: Sage publications, Newbury Park, London.

Miranda, S. M., & Saunders, C. S. (2003). The Social Construction of Meaning: An Alternative Perspective on Information Sharing. *Information systems research, 14*(1), 87-106. doi: 10.1287/isre.14.1.87.14765

Moore, T., & Clayton, R. (2007). *An empirical analysis of the current state of phishing attack and defence.* Paper presented at the the 2007 Workshop on The Economics of Information Security (WEIS2007).

Murphy, J. M. (2005). *The water is wide: network security at Kenyon College, 1995-2005*. Paper presented at the Proceedings of the 33rd annual ACM SIGUCCS fall conference, Monterey, CA, USA.

O'Keefe, D. J. (2002). *Persuasion: theory & research* (2 ed. Vol. 2): Sage Publications, Inc.

O'Malley, G. (2005). Jupiter Analyst: Nielsen Research Confirms Users Delete Cookies. Retrieved 10/9, 2009, from http://www.mediapost.com/publications/article/28883/jupiter-analyst-nielsen-research-confirms-users-d.html#axzz2KBM0FmTt

Oppliger, R., Hauser, R., & Basin, D. (2006). SSL/TLS session-aware user authentication--Or how to effectively thwart the man-in-the-middle. *Computer Communications, 29*(12), 2238--2246.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. http://www.swdsi.org/swdsi2009/Papers/9J05.pdf

Perloff, R. M. (2010). *The dynamics of persuasion: Communication and attitudes in the 21st century* (4 ed.): Taylor & Francis.

Pettey, C. (2006). Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008. Retrieved 2/9, 2009, from http://www.gartner.com/it/page.jsp?id=936913

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in experimental social psychology, 19*(1), 123-205.

Pfeiffer, T., Theuerling, H., & Kauer, M. (2013). Click Me If You Can! In L. Marinos & I. Askoxylakis (Eds.), *Human Aspects of Information Security, Privacy, and Trust* (Vol. 8030, pp. 155-166): Springer Berlin Heidelberg.

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security, 20*(5), 382 - 420.

Rexha, B. (2005, July). *Increasing user privacy in online transactions with X.509 v3 certificate private extensions and smartcards.* Paper presented at the E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on.

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS-SEM in MIS quarterly. *MIS Q., 36*(1), iii-xiv.

Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of Statistical, 48*(2), 1-36.

Rosseel, Y. (2013). The lavaan project. Retrieved 15/4/2013, from http://lavaan.ugent.be/tutorial/cat.html

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review, 23*(3), 393-404.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (5th ed. ed.). Harlow, U.K. :: Financial Times- Prentice Hall.

Sekaran, U. (2003). *Research methods for business : a skill-building approach* (4th ed.). New York :: John Wiley & Sons.

Sharma, K. (2010). An Anatomy of Phishing Messages as Deceiving Persuasion: A Categorical Content and Semantic Network Study. *EDPACS, 42*(6), 1-19. doi: 10.1080/07366981.2010.537191

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions*. Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems, Atlanta, Georgia, USA.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). *Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish*. Paper presented at the Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania.

Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., & Zhang, C. (2009). *An empirical analysis of phishing blacklists.* Paper presented at the Sixth Conference on Email and Anti-Spam (CEAS), CA, USA.

Shujun, L., & Schmitz, R. (2009). *A novel anti-phishing framework based on honeypots.* Paper presented at the eCrime Researchers Summit, 2009. eCRIME '09., Tacoma, WA, USA.

Silverman, D. (2006). *Interpreting qualitative data: methods for analyzing talk, text and interaction*. Thousand Oaks: Sage.

Smith, P. B. (2004). Acquiescent response bias as an aspect of cultural communication style. *Journal of Cross-Cultural Psychology, 35*(1), 50-61.

Srivastava, S., John, O. P., Gosling, S. D., & Potter, J. (2003). Development of personality in early and middle adulthood: set like plaster or persistent change? *Journal of personality and social psychology, 84*(5), 1041-1053.

Stebila, D. (2010). *Reinforcing bad behaviour: the misuse of security indicators on popular websites*. Paper presented at the Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction, Brisbane, Australia.

Stiff, J. B., Kim, H. J., & Ramesh, C. N. (1992). Truth biases and aroused suspicion in relational deception. *Communication Research, 19*(3), 326.

Sven, D., Rachna, D., Vivek, A., Andrew, D., Markus, J., Debin, L., & Heather, R. (2007). Phishing IQ Tests Measure Fear, Not Ability *Financial Cryptography and Data Security* (Vol. 4886, pp. 362-366): Springer Berlin / Heidelberg.

Teddlie, C., & Yu, F. (2007). Mixed methods sampling a typology with examples. *Journal of mixed methods research, 1*(1), 77-100.

Tembe, R., Hong, K. W., Murphy-Hill, E., Mayhorn, C., & Kelley, C. (2013). *American and Indian Conceptualizations of Phishing.* Paper presented at the Proceedings of the 3rd Workshop on Socio-Technical Aspects in Security and Trust.

Trenholm, S. (1989). *Persuasion and social influence*: Prentice Hall Englewood Cliffs, NJ.

Trusteer. (2009). Measuring the Effectiveness of In-the-Wild Phishing Attacks. http://www.opensourceintelligence.eu/ric/doc/Phishing-Statistics-Dec-2009-FIN.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. doi: 10.1016/j.dss.2011.03.002

Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). An Exploration of the Design Features of Phishing Attacks. *Information Assurance, Security and Privacy Services, 4*, 29.

Whitten, A. (2004). *Making security usable.* (PhD), Carnegie Mellon University, United States.

Williamson, G. D. (2006). Enhanced Authentication In Online Banking. *Journal of Economic Crime Management, 4*(2).

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59*(4), 329-349.

Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where Did They Go Right? Understanding the Deception in Phishing Communications. *Group Decision and Negotiation, 19*(4), 391-416. doi: 10.1007/s10726-009-9167-9

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). *Do security toolbars actually prevent phishing attacks?* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada.

Wu, M., Miller, R. C., & Little, G. (2006). *Web wallet: preventing phishing attacks by revealing user intentions.* Paper presented at the SOUPS '06: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA.

Wu, Y., Yao, H., & Bao, F. (2008). Minimizing SSO Effort in Verifying SSL Anti-phishing Indicators *Proceedings of The Ifip Tc 11 23rd International Information Security Conference* (Vol. 278, pp. 47-61): Springer US.

Xia, H., & Brustoloni, J. e. C. (2005). *Hardening Web browsers against man-in-the-middle and eavesdropping attacks.* Paper presented at the WWW '05: Proceedings of the 14th international conference on World Wide Web, New York, NY, USA.

Xun, D., Clark, J. A., & Jacob, J. (2008). *Modelling user-phishing interaction.* Paper presented at the Proceedings of Human System Interactions May 25-27, 2008, Kraków, Poland.

Ye, E., Yuan, Y., & Smith, S. W. (2002). Web spoofing revisited: SSL and beyond. *Computer Science Technical Report TR2001-417, Department of Computer Science, Dartmouth College*.

Yesser. (2013). E-government Program. 12/5/2013, from http://www.yesser.gov.sa/en/Pages/default.aspx

Yue, C., & Wang, H. (2008, 8-12 Dec. 2008). *Anti-Phishing in Offense and Defense.* Paper presented at the Computer Security Applications Conference, 2008. ACSAC 2008. Annual.

Zhang, W., Luo, X., Burd, S. D., & Seazzu, A. F. (2012). *How Could I Fall for That? Exploring Phishing Victimization with the Heuristic-Systematic Model*.

Appendices

Appendix A

Research survey

The survey for both experiments:

First survey:

Email has become a very important way of communication. Unfortunately, on a daily basis we receive emails which may not be useful or appropriate. We are currently doing a research which aims to help users filter out such emails. Specifically, this research investigates different aspects of various users' behaviour in their interaction with emails.

You can help us achieve this goal by answering these questions which will take approximately 15-20 minutes. This research comprises two surveys in which this survey is the first. The second survey will be sent to you at a later date.

1. Age:

☐(18-25) ☐(26-35) ☐(36 and above)

2. Gender:

☐Male ☐Female

3. First Language:[11]

☐English ☐Other

4. Nationality:[12]

☐Australian ☐Other

[11] Not applicable in Saudi Arabia because all participants have Arabic as their first language
[12] Not applicable in Saudi Arabia because all participants have Saudi Arabian nationality

5. Please circle the corresponding number in each statement which best describes the degree to which a statement is **true** for you:

Strongly disagree	Moderately disagree	Disagree a little	Neither agree nor disagree	Agree a little	Moderately agree	Strongly agree
1	2	3	4	5	6	7

Big Five Personality Dimensions Variables

I see myself as:

• Extroverted, enthusiastic	1	2	3	4	5	6	7
• Critical, quarrelsome	1	2	3	4	5	6	7
• Dependable, self-disciplined	1	2	3	4	5	6	7
• Anxious, easily upset	1	2	3	4	5	6	7
• Open to new experiences, complex	1	2	3	4	5	6	7
• Reserved, quiet	1	2	3	4	5	6	7
• Sympathetic, warm	1	2	3	4	5	6	7
• Disorganized, careless	1	2	3	4	5	6	7
• Calm, emotionally stable	1	2	3	4	5	6	7
• Conventional, uncreative	1	2	3	4	5	6	7

Trust Variable

• I usually trust people until they give me a reason not to trust them	1	2	3	4	5	6	7
• I generally give people the benefit of the doubt when I first meet them	1	2	3	4	5	6	7
• My typical approach is to trust new acquaintances until they prove I should not trust them	1	2	3	4	5	6	7

Submissiveness Variable

6. Please circle the corresponding number in each statement which best describes the degree to which a statement is **true** for you:

Never	Rarely	Sometimes	Mostly	Always
1	2	3	4	5

• I agree that I am wrong even though I know I'm not	1	2	3	4	5
• I do things because other people are doing them, rather than because I want to	1	2	3	4	5
• I would walk out of a shop without questioning, knowing that I had been short changed	1	2	3	4	5
• I let others criticise me or put me down without defending myself	1	2	3	4	5
• I do what is expected of me even when I don't want to	1	2	3	4	5

• If I try to speak and others continue, I shut up	1	2	3	4	5
• I continue to apologise for minor mistakes	1	2	3	4	5
• I listen quietly if people in authority say unpleasant things about me	1	2	3	4	5
• I am not able to tell my friends when I am angry with them	1	2	3	4	5
• At meetings and gatherings, I let others monopolise the conversation	1	2	3	4	5
• I don't like people to look straight at me when they are talking	1	2	3	4	5
• I say 'thank you' enthusiastically and repeatedly when someone does a small favour for me	1	2	3	4	5
• I avoid direct eye contact	1	2	3	4	5
• I avoid starting conversations at social gatherings	1	2	3	4	5
• I blush when people stare at me	1	2	3	4	5
• I pretend I am ill when declining an invitation	1	2	3	4	5

Internet usage

7. How many years you have been using the Internet?

☐ Number of years

8. How many hours you usually spend in the Internet per day?

☐ Number of hours

For Australian survey Internet activities 1, 2 and 3

9. On average, how much time per week do you spend on each of the following Web activities?

None	1-30 Min	30-60 Min	1-2 Hours	2-4 Hours	4-8 Hours	More than 8
1	2	3	4	5	6	7

• Surfing the Internet for knowledge (read only)	1	2	3	4	5	6	7
• Making social activities (communicating with others)	1	2	3	4	5	6	7
• Making online transactions (shopping – banking)	1	2	3	4	5	6	7

For Saudi survey Internet activities 1, 2 and 3

10. You mainly use the Internet for: (Tick all that applies)

☐ Surfing the Internet for knowledge (read only)
☐ Making social activities (communicating with others)
☐ Making online transactions (shopping – banking)

Email usage

11. How many years you have been using the email service?

☐ Number of years

12. How many years you have been using university email service?

☐ Number of years

13. What is the average number of emails you normally receive per day in your inboxes:

☐ Number of emails

Perceived email Experience and Richness Variables

14. Please circle the corresponding number in each statement which best describes the degree to which a statement is **true** for you:

Strongly disagree	Moderately disagree	Disagree a little	Neither agree nor disagree	Agree a little	Moderately agree	Strongly agree
1	2	3	4	5	6	7

Perceived email Experience Variable

• I am very experienced using e-mail	1	2	3	4	5	6	7
• I feel that e-mail is easy to use	1	2	3	4	5	6	7
• I feel competent using e-mail	1	2	3	4	5	6	7
• I understand how to use all of the features of the e-mail system	1	2	3	4	5	6	7
• I feel comfortable using e-mail	1	2	3	4	5	6	7
• I feel that I am a novice using the e-mail system	1	2	3	4	5	6	7

Perceived Email Richness Variable

• E-mail allows my communication partner and me to give and receive timely feedback	1	2	3	4	5	6	7
• E-mail allows my communication partner and me to tailor our messages to our own personal requirements	1	2	3	4	5	6	7
• E-mail allows my communication partner and me to communicate a variety of different cues (such as emotional tone, attitude, or formality) in our messages	1	2	3	4	5	6	7
• E-mail allows my communication partner and me to use rich and varied language in our messages	1	2	3	4	5	6	7

Susceptibility Variable

15. Please read this short paragraph to answer this question

Mr. John Douglas is a student at QUT University. He often shops from the Internet for which he uses his PayPal and eBay accounts. John verifies transactions done by PayPal using his online bank statement as he banks with commonwealth bank of Australia. These organisations send emails about updates done on John's account and status. John always checks his email inbox and reads emails from QUT, Commonwealth Bank, PayPal and eBay.

Dear participant, please pretend that you are John Douglas with the email address john@yahoo.com.au and you received the next three emails. The question is how likely that you will click on the link included in these emails. Rate your answer from 1 to 7 where:

1	Definitely will delete or ignore the email	5	Maybe will respond
2	Most likely will delete or ignore the email	6	Most likely will respond
3	Maybe will delete or ignore the email	7	Definitely will respond
4	I do not Know		

Email 1 (Scam):
Answer: 1 2 3 4 5 6 7

Email 2(University email):
Answer: 1 2 3 4 5 6 7

Email 3(PayPal):
Answer: 1 2 3 4 5 6 7

Email 4 (eBay):
Answer: 1 2 3 4 5 6 7

Email 5 (Bank):
Answer: 1 2 3 4 5 6 7

Second survey:

This survey tries to capture the process that you have done when you received the phishing email used in our research. This survey will takes from 2 to 5 minutes from your valuable time.

16. Did you see this email

Image of the phishing email

☐Yes ☐No

Confirmation Channel (Channel) Variable

17. What did you do to check the authenticity of the email?: (Tick all that applies)

☐ Asking other persons face-to-face
☐ Asking other persons by Telephone
☐ Asking other persons by email
☐ Make a decision by yourself without consulting others
☐ Other:

Appendix B

Interview questions

1. Have you heard about phishing emails?
2. How do you identify phishing emails?
3. Can you please explain the situation when you received our phishing email?
4. What did you do when you opened the phishing email? Why?
5. Have you checked the links in the phishing email? What did you found?
6. Have you checked the reply address in the phishing email? What did you found?
7. What did you do when you suspected the phishing email?
8. Why did you respond to the phishing email? (for victims)
9. What did you do when you discover the phishing email? (for detectors)
10. What is your reaction if someone accesses your account?
11. How important is your account to you?

Appendix C

Information sheet

Queensland University of T Brisbane Australia	PARTICIPANT INFORMATION FOR QUT RESEARCH PROJECT – Interview –

Distinguishing between detectors and non-detectors of phishing emails

QUT Ethics Approval Number 1100001164

RESEARCH TEAM

RESEARCH TEAM INFORMAITON

DESCRIPTION

This project is being undertaken as part of PhD project for Mr Ibrahim Alseadoon at QUT. The purpose of this project is to find important characteristics in Internet users which make them to respond to phishing emails. The main aim of phishing emails is to gain access to your secret personal information.

This project also aims to find the impact of users characteristics on their detection decision. The outcome of this research will help in identifying users who are more likely to be vulnerable to phishing emails. Finding these users will help to improve their defences against phishing emails. Furthermore, this research will help in classifying users using their characteristics to draw the line for security designers to design special security tools for users, based on the variety of users' characteristics. You are invited to participate in this project because you responded to a phishing email. Please be assured that this is a common occurrence, and your experience is valuable to us and may prevent other users from responding to these harmful emails.

PARTICIPATION

Your participation in this project is entirely voluntary. If you do agree to participate you can withdraw from the project without comment or penalty. If you withdraw, on request any identifiable information already obtained from you will be destroyed. Your decision to participate or not participate will in no way impact upon your current or future relationship with QUT.

Your participation will involve an audio recorded interview (optional) at my office XXX or other agreed location that will take approximately 20 to 30 minutes of your time. Questions will include the reasons why you responded to the email, the time of the email and your email experience.

EXPECTED BENEFITS

It is expected that this project will not directly benefit you immediately. However, it may benefit you by improving security and defences against phishing emails in the near future in order to make this world a better place for providing secure online services as well as protecting users from phishing attacks.

To recognise your contribution should you choose to participate the research team is offering you a XXX Coffee voucher.

RISKS

There are no risks beyond normal day-to-day living associated with your participation in this project.

PRIVACY AND CONFIDENTIALITY

All comments and responses will be treated confidentially and will not be used outside this research project. Also, your name will be replaced with numbers during the research to protect your privacy. Non-identifiable data collected in this project may also be used as comparative data in future projects.

The project is funded by Saudi Arabian Government however they will not have access to the data

obtained during the project and all private information will be protected during this research.

CONSENT TO PARTICIPATE

We would like to ask you to sign a written consent form to confirm your agreement to participate.

QUESTIONS / FURTHER INFORMATION ABOUT THE PROJECT

If you have any questions or require any further information please contact one of the research team members below.

RESEARCH TEAM INFORMAITON

CONCERNS / COMPLAINTS REGARDING THE CONDUCT OF THE PROJECT

QUT is committed to research integrity and the ethical conduct of research projects. However, if you do have any concerns or complaints about the ethical conduct of the project you may contact the QUT Research Ethics Unit on 3138 5123 or email ethicscontact@qut.edu.au. The QUT Research Ethics Unit is not connected with the research project and can facilitate a resolution to your concern in an impartial manner.

Thank you for helping with this research project. Please keep this sheet for your information.

Appendix D

Consent form

Queensland University of Te Brisbane Australia	CONSENT FORM FOR QUT RESEARCH PROJECT – Interview –
Distinguishing between detectors and non-detectors of phishing emails	
QUT Ethics Approval Number 1100001164	

RESEARCH TEAM CONTACTS

RESEARCH TEAM INFORMAITON

STATEMENT OF CONSENT

By signing below, you are indicating that you:

- Have read and understood the information document regarding this project.
- Have had any questions answered to your satisfaction.
- Understand that if you have any additional questions you can contact the research team.
- Understand that you are free to withdraw at any time, without comment or penalty.
- Understand that you can contact the Research Ethics Unit on 3138 5123 or email ethicscontact@qut.edu.au if you have concerns about the ethical conduct of the project.
- Understand that non-identifiable data collected in this project may be used as comparative data in future projects.
- Agree to participate in the project.

Please tick the relevant box below:

☐ I agree for the interview to be audio recorded.

☐ I do not agree for the interview to be audio recorded.

Name

Signature

Date

Please return this sheet to the investigator.